

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2003年9月4日 (04.09.2003)

PCT

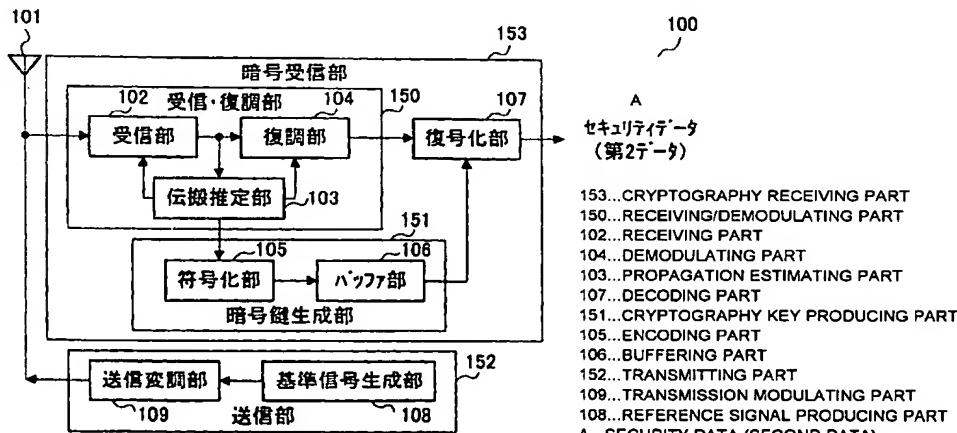
(10) 国際公開番号
WO 03/073689 A1

- (51) 国際特許分類7:
9/14, H04Q 7/38, H04B 7/06 H04L 9/08, 二俣 1-12-1-302 Chiba (JP). 村上 豊 (MURAKAMI,Yutaka) [JP/JP]; 〒213-0034 神奈川県 川崎市 高津区 上作延532-1-201 Kanagawa (JP). 安倍 克明 (ABE,Katsuaki) [JP/JP]; 〒215-0005 神奈川県 川崎市麻生区 千代ヶ丘8-21-13-F201 Kanagawa (JP). 松岡 昭彦 (MATSUOKA,Akihiko) [JP/JP]; 〒226-0021 神奈川県 横浜市 緑区 北八朔町2108-1-201 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP03/02174 (74) 代理人: 鷲田 公一 (WASHIDA,Kimihito); 〒206-0034 東京都 多摩市 鶴牧1丁目24-1 新都市センタービル 5階 Tokyo (JP).
- (22) 国際出願日: 2003年2月27日 (27.02.2003) (81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (25) 国際出願の言語: 日本語 (84) 指定国(広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-54064 2002年2月28日 (28.02.2002) JP
特願2002-132068 2002年5月7日 (07.05.2002) JP
特願2003-48364 2003年2月25日 (25.02.2003) JP
- (71) 出願人(米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 折橋 雅之 (ORIHASHI,Masayuki) [JP/JP]; 〒272-0001 千葉県市川市

[統葉有]

(54) Title: COMMUNICATION APPARATUS AND COMMUNICATION SYSTEM

(54) 発明の名称: 通信装置及び通信システム



(57) Abstract: A propagation estimating part (103) uses a reference signal of propagation estimation, sent from the other end of communication, to estimate a propagation environment. This estimation result is sent, as propagation information for reception/de-modulation parameters, to a receiving part (102) and a demodulating part (104), thereby removing multipath components from a received signal or performing phase adjustment and the like, in accordance with the propagation information, to output demodulated information.

[統葉有]

WO 03/073689 A1



特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

2 文字コード及び他の略語については、定期発行される
各 PCT ガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

添付公開書類:
— 國際調査報告書

(57) 要約:

本発明は、通信相手から送られてきた伝搬推定用の基準信号を用いて伝搬推定部 103 で伝搬環境を推定し、その推定結果を受信復調バラメータ用に伝搬情報として受信部 102、復調部 104 へと送出され前記伝搬情報に従って受信信号からマルチパス成分を除去、或いは位相の調整などを行いながら復調情報を出力する。

明細書

通信装置及び通信システム

5 技術分野

本発明は、ディジタル通信に用いられる技術であって、特にセキュリティ技術に関する。

背景技術

10 ディジタル無線通信は、その技術の発展により通信分野の重要な位置を占めるようになってきている。しかしながら、無線通信が公共財である電波空間を利用したものであるため、第3者による受信が可能であるといった根本的な課題を内包している。このため、常に通信内容が第3者により傍受され、情報が漏洩する危険性をはらんでいる。

15 このような問題を解決するために、通信情報を暗号化するなどして傍受されても情報が漏洩しないような処理を行っているのが現状である。

情報の暗号化は、様々な分野で研究され、また様々な分野で応用されている。これは、通信システムを変更しなくとも一定のセキュリティが確保できるといった大きな特長によるところが大きい。

20 しかしながら、通信情報を暗号化しても第3者による傍受を防ぐことはできないため、第三者により傍受された受信情報から時間をかけることにより暗号化した通信情報が解読されてしまうと言った問題がある。

発明の開示

25 本発明の目的は、大きな通信システムの変更をすることなしに高いセキュリティを確保することである。

この目的は、通信相手から送信された基準信号を用いて推定した伝搬環境の

情報を秘匿情報として取得することにより達成できる。

図面の簡単な説明

- 図 1 は、本発明の実施の形態 1 に係る通信装置の構成を示すブロック図、
5 図 2 は、本発明の実施の形態 1 に係る通信装置の構成を示すブロック図、
図 3 は、本発明の実施の形態 1 に係る通信装置の動作を示すシーケンス図、
図 4 は、本発明の実施の形態 2 に係る通信装置における伝搬推定部と符号化
部の構成を示すブロック図、
図 5 は、コードブックを示す図、
10 図 6 は、遅延プロファイルを示す図、
図 7 は、本発明の実施の形態 3 に係る通信装置の構成を示すブロック図、
図 8 は、本発明の実施の形態 3 に係る通信装置の動作を示すシーケンス図、
図 9 は、本発明の実施の形態 4 に係る通信装置の構成を示すブロック図、
図 10 は、本発明の実施の形態 4 に係る通信装置の構成を示すブロック図、
15 図 11 は、本発明の実施の形態 5 に係る通信装置の動作を示すシーケンス図、
図 12 は、本発明の実施の形態 6 に係る信号のフレーム構成を示す図、
図 13 は、本発明の実施の形態 6 に係る信号のフレーム構成を示す図、
図 14 は、本発明の実施の形態 7 に係る通信装置の構成を示すブロック図、
図 15 は、本発明の実施の形態 7 に係る通信装置の構成を示すブロック図、
20 図 16 は、本発明の実施の形態 8 に係る通信装置における伝搬推定部の構成
を示すブロック図、
図 17 は、到来方向推定結果を説明する図、
図 18 は、本発明の実施の形態 9 に係る通信装置の構成を示すブロック図、
図 19 は、偏波状態を説明する図、
25 図 20 は、本発明の実施の形態 10 に係る通信装置の構成を示すブロック図、
図 21 は、本発明の実施の形態 11 に係る通信装置の構成を示すブロック図、
図 22 は、本発明の実施の形態 12 に係る通信装置の構成を示すブロック図、

図23は、本発明の実施の形態13に係る通信装置の構成を示すブロック図、

図24は、本発明の実施の形態13に係る通信装置の構成を示すブロック図、

図25は、本発明の実施の形態13に係る通信装置の動作を示すシーケンス図、

5 図26は、本発明の実施の形態14に係る通信装置の構成を示すブロック図、

図27は、本発明の実施の形態14に係る通信装置における伝搬推定部の構

成を示すブロック図、

図28は、自己相関系列を示す図、

図29は、遅延プロファイルを示す図、

10 図30は、本発明の実施の形態15に係る通信装置における伝搬推定部の構成を示すブロック図、

図31は、本発明の実施の形態16に係る通信装置の構成を示すブロック図、

図32は、本発明の実施の形態16に係る通信装置における伝搬推定部、変換部及び符号化部の構成を示すブロック図、

15 図33は、本発明の実施の形態16に係るシステムブロック図、

図34は、遅延プロファイルの周波数特性を示す図、

図35は、本発明の実施の形態17に係る通信装置の構成を示すブロック図、

図36は、本発明の実施の形態17に係る通信装置の構成を示すブロック図、

図37は、本発明の実施の形態17に係る通信装置の動作を示すシーケンス

20 図、

図38は、本発明の実施の形態17に係る通信装置の信号処理を示す図、

図39は、本発明の実施の形態17に係る通信装置の信号処理を示す図、

図40は、電力分布を示す図、

図41は、電力分布を示す図、

25 図42は、電力分布を示す図、

図43は、本発明の実施の形態18に係る通信装置の構成を示すブロック図、

図44は、本発明の実施の形態18に係る通信装置の構成を示すブロック図、

- 図45は、本発明の実施の形態18に係る通信装置の信号処理を示す図、
図46は、本発明の実施の形態19に係る通信装置の構成を示すブロック図、
図47は、本発明の実施の形態19に係る通信装置の動作を示すシーケンス
図、
5 図48は、本発明の実施の形態20に係る信号のフレーム構成を示す図、
図49は、本発明の実施の形態20に係る信号のフレーム構成を示す図、
図50は、本発明の実施の形態21に係る信号のフレーム構成を示す図、
図51は、本発明の実施の形態22に係る通信装置の構成を示すブロック図、
図52は、本発明の実施の形態22に係る信号のフレーム構成を示す図、
10 図53は、本発明の実施の形態23に係る通信装置の構成を示すブロック図、
図54は、本発明の実施の形態23に係る信号のフレーム構成を示す図、
図55は、本発明の実施の形態24に係る通信装置の構成を示すブロック図、
図56は、本発明の実施の形態24に係る通信装置の構成を示すブロック図、
図57は、本発明の実施の形態25に係る通信装置の構成を示すブロック図、
15 図58は、本発明の実施の形態25に係る通信装置の構成を示すブロック図、
図59は、本発明の実施の形態27に係る通信装置を用いた通信システムを
示す図、
図60は、本発明の実施の形態27に係る通信装置の構成を示すブロック図、
20 図61は、本発明の実施の形態27に係る通信装置の動作を示すシーケンス
図、
図62は、本発明の実施の形態27に係る通信装置の動作を示すシーケンス
図、
図63は、本発明の実施の形態27に係る通信装置の動作を示すシーケンス
図、
25 図64は、信号の送信状態を時間軸で示した図、
図65は、信号の送信状態を時間軸で示した図、
図66は、信号の送信状態を時間軸で示した図、

図 6 7 は、信号の送信状態を時間軸で示した図、

図 6 8 は、本発明の実施の形態 2 6 に係る通信装置を用いた通信システムを示す図、

図 6 9 は、本発明の実施の形態 2 6 に係る通信装置を用いた通信システムを
5 示す図、

図 7 0 は、本発明の実施の形態 2 6 に係る通信装置を用いた通信システムを示す図、

図 7 1 は、電力分布を示す図、

図 7 2 は、伝搬パラメータの直交性の時間的変化を示す図、

10 図 7 3 は、通信品質をビットエラーレート（B E R）で表した図、

図 7 4 は、通信品質をビットエラーレート（B E R）で表した図、

図 7 5 は、信号の送信状態を時間軸で示し図、

図 7 6 は、電力分布を示す図、

図 7 7 は、本発明の実施の形態 2 8 に係る通信装置を用いた通信システムを
15 示す図、及び

図 7 8 は、本発明の実施の形態 2 8 に係る通信装置の受信処理を示した図である。

発明を実施するための最良の形態

20 以下、本発明の実施の形態について図面を用いて説明する。

（実施の形態 1）

伝搬情報をセキュリティの暗号鍵情報として利用する発明について図 1、図 2 および図 3 を用いて説明する。図 1 は本実施の形態 1 に係る通信装置である暗号受信装置の具体的構成を示し、図 2 は暗号送受信装置の具体的構成を示したものである。図 3 は端末間の通信手続きを記述したものである。ここでは便宜上、図 3 中の基地局を図 2 に示した暗号送受信装置、端末を図 1 で示した暗号受信装置であるものとして説明を行うが、その組合せを制限するものではない

く、両者が図2で示す暗号送受信装置であっても構わない。

図1はアンテナ101と、暗号受信部153と、送信部152とで構成されている。暗号受信部153は受信したRF信号から伝搬状態を推定し、これを暗号鍵として暗号の復号を行いセキュリティデータを出力するものであり、受信復調部150と、暗号鍵生成部151と、復号化部107とで構成されている。送信部152は基準RF信号を出力するものであり、基準信号生成部108、送信変調部109とからなる。アンテナ101は電波を受信・送信しRF信号を入出力するものであり、受信復調部150はRF信号を入力し、伝搬情報と復調情報を出力するものであり、受信部102、伝搬推定部103、復調部104とからなる。

受信部102はRF信号と伝搬情報を入力し、RF信号を適切な受信状態に制御し、受信信号を出力するものであり、伝搬推定部103は受信信号から伝搬特性を推定し伝搬情報を出力するものであり、復調部104は受信信号と伝搬情報とから適切な復調を行い復調情報を出力するものである。暗号鍵生成部151は伝搬情報を入力し暗号鍵情報を出力するものであり、符号化部105とバッファ部106とで構成されている。

符号化部105は伝搬情報から特徴を抽出し暗号鍵（第1データ）を生成・出力するものであり、バッファ部106は符号化された暗号鍵を記憶し、記憶した暗号鍵情報を出力するものである。復号化部107は暗号鍵情報と復調情報とを入力し、暗号鍵情報から復調情報の暗号を復号化しセキュリティデータ（第2データ）を出力するものである。基準信号生成部108は予め定められた基準信号を生成し出力するものであり、送信変調部109は基準信号を入力しRF信号に変調・出力するものである。

図2はアンテナ201と、暗号受信部253と、暗号送信部254とで構成されている。アンテナ201および暗号受信部253は、図1中での対応する部位と同等の機能を有している。暗号送信部254はセキュリティデータと暗号鍵情報を入力し、伝搬推定用の基準信号と、暗号鍵情報とセキュリティデ

ータとから予め定められた方法により暗号化される暗号化情報と、を切り換えて変調・出力するものであり、送信変調部 252 と、基準信号生成部 208 と、暗号化部 209 と、切換部 210 とで構成される。

送信変調部 252 は選択された通信情報を変調し RF 信号を出力するもの 5 であり、変調部 211 と送信部 212 とから構成されている。基準信号生成部 208 は予め定められた基準信号を生成し出力するものであり、暗号化部 20 9 は暗号鍵情報とセキュリティデータとを入力し、暗号鍵情報からセキュリティデータを暗号化し、暗号情報を生成・出力するものである。切換部 210 は 10 基準信号と暗号情報を入力し、両者のうち 1 つを選択、通信情報を出力するものであり、変調部 211 は選択された通信情報を変調し変調信号を出力するものであり、送信部 212 は変調信号を送信する RF 信号に変換・出力するものである。

以上のように構成された基地局(図 2 に示される暗号送受信装置)と端末(図 1 に示される暗号受信装置を含む通信装置)とは、図 3 のような手順で通信を行っている。

以下、図 1 に示された装置の動作を説明する。アンテナ 101 は、電波を受信し RF 信号を出力する。受信された RF 信号は、受信復調部 150 に入力され伝搬情報と復調情報とが output される。まず、受信部 102 は RF 信号と伝搬情報を入力し、伝搬情報に従い、ゲインを一定に保つたり、周波数・時間ずれ 20 を修正したりすることで受信状態を最適に保つように制御しながら受信信号を出力する。伝搬推定部 103 は受信信号を入力し、受信時刻、伝搬時間、周波数状態、偏波状態、受信電力、マルチパス状態、位相状態、伝搬歪などを検出する。

それぞれの状態は、受信復調パラメータ用に伝搬情報として受信部 102、 25 復調部 104 へと送出されると同時に、暗号鍵生成部 151 へも送出される。復調部 104 は、受信信号と伝搬情報を入力し、伝搬情報に従って受信信号からマルチパス成分を除去、或いは位相の調整などを行いながら復調し、復調

情報を出力する。暗号鍵生成部 151 は受信復調部 150 から出力された伝搬情報から伝搬状態の特徴を抽出し、暗号鍵を生成・記憶し、暗号鍵情報を出力する。

符号化部 105 は伝搬推定部 103 から出力された伝搬情報を入力し、その
5 中から受信信号の伝搬状態の特徴を抽出する。例えば、マルチバス状態を例に挙げると、複数の伝搬路により形成されるマルチバス伝搬において、そのマルチバス特性は相関関数などを用いて検出することが可能である。

このようにして求められたマルチバスの電界情報のうち、最大のパワーを検出したパス成分の遅延時間とパワーとから予め定められた方法に従って符号
10 化を行い、暗号化に用いる暗号鍵を生成・出力する。生成された暗号鍵は、バッファ部 106 で入力され記憶されて、暗号鍵情報が outputされる。復号化部 107 は、復調情報と暗号鍵情報を入力し予め定められた方法に従って復調情報を復号し、セキュリティデータを出力する。送信部 152 は基準信号を生成した後、変調し RF 信号を出力する。基準信号生成部 108 は、通信対象の相手
15 端末に対して伝搬状態を推定するための基準信号を生成し、これを出力する。送信変調部 109 は基準信号を入力し、変調・周波数変換などにより RF 信号を出力する。出力された RF 信号は、アンテナ 101 から放射される。

次に、図 2 に示された装置の動作を説明する。ここでは、図 1 に示した装置からの相違点のみを示す。

20 アンテナ 201 から入力された RF 信号が、復号化部 207 を通じて復号されセキュリティデータが出力されるまでの暗号受信部 253 は、図 1 の対応する部位と同一の構成である。暗号送信部 254 は、暗号鍵情報とセキュリティデータを入力し、送信する RF 信号を出力する。基準信号生成部 208 は、通信対象の相手端末に対して伝搬状態を推定するための基準信号を生成し、出力
25 する。暗号化部 209 は、暗号鍵情報とセキュリティデータとを入力し、予め定められた方法に従って暗号化した暗号化情報を出力する。

切換部 210 は、基準信号生成部 208 から入力される基準信号と、暗号化

部 209 から入力される暗号化情報の一方を選択し選択された通信情報を出力する。選択された通信情報は、送信変調部 252 により変調され送信信号に変換されて R F 信号を出力する。即ち、通信情報は、変調部 211 に入力され所定の変調が施されて変調部 211 より変調信号として出力される。次に、変 5 調信号は、送信部 212 へ入力され、R F 信号に変換されて送信部 212 より出力される。この R F 信号はアンテナ 201 を介して放射される。

以上の動作を、通信手順の観点から図 3 を用いて説明する。

(0) 基地局、端末：初期化

基地局、端末共に、電源が投入された直後、或いは特定の信号を受けて初期 10 状態にセットされる。同時に、周波数や時間同期などの状態は事前に定められた手順に従ってセットされる。

以上のこれらの初期動作が終了した一定時間後、基地局は一定時間毎に制御 情報を制御信号に載せて送信する。

一方、端末は初期動作が終了した後、制御信号のサーチを始める。端末が基 15 地局から送信した制御信号を受信すると、その時刻、周波数などを検出してシ ステムが保有する時刻・周波数に同期する（システム同期）。システム同期が 正常に終了した後、端末はその存在を基地局に通知するために登録要求信号を 送信する。基地局は、端末からの登録要求に対して、登録許可信号を送信する ことで端末の登録許可を行う。

20 (1) 基地局：第 1 基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第 1 基準信号として出力する。 具体的には、切換部 210 は基準信号生成部 208 で生成される基準信号を選 択し、送信変調部 252 へ出力する。送信変調部 252 は選択された通信情報 を R F 信号としてアンテナ 201 から放射する。

25 端末では、基地局からの信号を待っており、伝搬推定部 103 は受信した受 信信号から第 1 基準信号を検出し、受信信号と既知信号である基準信号とから 伝搬推定を行う。符号化部 105 は、伝搬推定部 103 からの伝搬情報を入力

し、伝搬状態の特徴抽出をおこなう。次に抽出した特徴情報を用いて暗号鍵への変換を行う。この部分の動作は別途詳細に説明する。この符号化部 105 が抽出する特徴や、それを暗号鍵へ変換する方法については基地局と端末の間で予め共有しておくものとする。変換された暗号鍵はバッファ部 106 に保持され暗号鍵情報が出力される。この暗号鍵を第 1 鍵として基地局は以降の通信の暗号鍵とする。

(2) 端末：第 2 基準信号送信

端末は、(1) と同様に基地局で行う伝搬推定用の基準信号を第 2 基準信号として出力する。

10 基地局では、端末からの信号を受信すると第 2 基準信号を検出し、伝搬推定部 203 は受信信号と既知信号である基準信号とから伝搬推定を行う。(1) と同様、伝搬推定部 203 が output する伝搬情報は、符号化部 205 によって暗号鍵へと変換され、バッファ部 206 で暗号鍵情報が保持、出力される。この暗号鍵を第 2 鍵として端末は以降の通信の暗号鍵とする。

15 (3) 基地局：暗号送信

基地局は、切換部 210 の状態を、暗号化部 209 から出力される暗号化情報を選択するように切り換える。暗号化部 209 は(2) で得られた第 2 鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化情報を出力する。暗号化情報は切換部 210 で選択され、通信情報が送信変調部 252 へと出力される。送信変調部 252 は通信情報を変調し、R.F. 信号としてアンテナ 201 から暗号化信号を放射する。

20 端末は、暗号化信号を受信すると受信復調部 150 が受信信号を復調情報へと復調する。復号化部 107 は復調情報と(1) で求めた第 1 鍵を用い、予め定められた方法によって暗号の復号化を行いセキュリティデータを出力する。25 以下、(3) の暗号通信や通常の通信を繰り返す。

さて、通信端末間で形成される伝搬路はその相対的な位置や空間形状、反射物などにより一意に決まり、それは基地局から端末に対して形成される伝搬状

態と、端末から基地局に対して形成される伝搬状態は光伝搬の相反性により同一であることが知られている。このことは、(1)で求められる伝搬状態と(2)で求められる伝搬状態（例えば、遅延プロファイルなど）は同一の結果が求まることとなることがわかる。また、基地局と端末の間では、予め伝搬情報から

5 暗号鍵へ変換する手順を共有してある。則ち、(1)で得られる暗号鍵（第1鍵）と(2)で得られた暗号鍵（第2鍵）は同一となり、通信端末間においては共有鍵として用いることが可能な状態となっている。この結果、(3)の通信手順においては共有鍵で暗号化・復号化を行うこととなり、基地局で暗号化された情報は端末で正常に復号化されることになる。

10 この状況で全通信を第3者が第3の端末を用いて傍受した場合を考える。先に説明したとおり、伝搬路は基地局と端末との間で形成される伝搬空間で求まるものである。このため、基地局や端末から物理的に異なった位置で(1)から(3)までの通信を観察している場合、第3の端末と基地局或いは端末間で形成される伝搬特性は、(1)や(2)で求められるそれとは異なってくる。

15 その上、基地局と端末間では暗号化の為の鍵の授受を行っているわけではないため、第3の端末がこれを知ることは出来ない。

このことから、通信の物理層において高いセキュリティを確保できることが分かる。また、これらの処理は基本的に従来の算術的な手法を用いた暗号化、復号化とは独立して行うことが可能であるため、従来技術に加えて本発明を実施することにより高いセキュリティが期待できるといった有利な特長を有する。

この説明において、初期化作業である(0)について説明を行ったが、これは一般的な運用を想定したものであり、本発明に必要な手続きではない。

また、(1)や(2)で基準信号を送信することで、互いの伝搬状態を推定するとしたが、これは一般に既知信号としての基準信号を用いた方が精度を高く推定できるためであって、伝搬推定では特に基準信号を用いなくても可能なことはいうまでもない。換言すれば、例えば(0)で行っている制御信号、登

録要求信号や登録許可信号などを利用して伝搬推定を行うことも可能である。

以上の発明は、伝搬状態を暗号鍵として利用することを特徴としているため、基地局や端末の移動が発生すると、問題が生ずる虞がある。この場合、図3に示した(1')、(2')、(3')のように繰り返し基準信号の送受信を行
5 うことで、この問題を回避することも可能である。

このように、本実施の形態1の通信装置及び通信システムによれば、伝搬推定部103が基準信号に基づいて伝搬環境を推定して相関関数等の伝搬パラメータである推定値を出力するとともに、符号化部105は推定値より得られたデータを出力するので、基地局と端末間で暗号化の為の鍵の授受を行う必要
10 がないために第3の端末がこれを知ることは出来ず、通信の物理層において大きな通信システムの変更をすることなしに高いセキュリティを確保することができる。また、本実施の形態1の通信装置及び通信システムによれば、従来の算術的な手法を用いた暗号化、復号化とは独立した処理によりセキュリティ
15 を確保することができるので、従来の暗号化、復号化技術と併用することにより極めて高いセキュリティを確保することができる。また、本実施の形態1の通信装置及び通信システムによれば、伝搬状態に応じて符号化パターンを変化させることができるので、環境変化に強い通信を行うことができる。また、本実施の形態1の通信装置及び通信システムによれば、推定した伝搬環境より伝
20 搬パラメータを求めて暗号鍵を取得することができるので、無変調の信号によって情報を送受信することができる。

なお、本実施の形態1においては、バッファ部106から出力される暗号鍵情報を復号化部107にてセキュリティデータを復号化する際の暗号鍵として用いることとしたが、これに限らず、バッファ部106から出力される暗号鍵情報を復号化部107にて復号化されるセキュリティデータ以外の他のセ
25 キュリティデータを復号化する際の暗号鍵として用いても良い。この場合には、復号化部107は不要になる。また、本実施の形態1においては、伝搬状態を示すパラメータとして遅延プロファイルを用いたが、偏波面や旋回方向などの

偏波状態を用いたり、位相情報を用いたり、伝搬遅延時間用いたり、到来方向推定情報を用いたり、受信電力情報を用いたり、或いは、様々なパラメータの組み合わせを用いたりすることも考えられる。こうすることで、第3の端末の観測がより複雑化するため高度なセキュリティを確保できる。特に、偏波や
5 位相を用いることで、それらが伝搬環境に大きく左右されることから、他の端末からの推定を一層困難にするといった特徴を有する。

さらに、複数のアンテナ 201 に複数のアンテナエレメントで構成するアレイアンテナ構造を適用することで、伝搬推定のパラメータとして到来方向の要素を付加することができる。こうすることでより柔軟なシステムを構成が可能
10 となる。

また、上記においては、変調方式、多重化方式について説明していないが、本方式は原理的にどの変調方式にも適用できることは明白であり、現在行われている P S K 変調、Q A M 変調、スター Q A M 変調、或いは T D M A 、 F D M A 、 S S (F H や C D M A) 、 O F D M 、あるいは空間多重 (S D M や M I M O) などあらゆるものに適用可能である。
15

さらに、通信手順で、基準信号を送信する際、第1基準信号の送信と第2基準信号の送信を行っているが、両者はどちらが先に実施されても本方式に影響を与えるものではないことは明白である。また、通信手順の中で基準信号を別途通信しているが、これは、後述する図 12 のフレーム構成 (b) 、 (c) の
20 ように、データストリームの中に基準信号を挿入することで、(1) と (3) の手順を同時に実施することができるといった有利な特長を有することが出来る。

(実施の形態 2)

本実施の形態 2 に係る通信装置は、伝搬推定と暗号鍵への変換方法について
25 説明するものであり、図 1 に示す本発明の実施の形態 1 に係る通信装置 100 において、伝搬推定部 103 と符号化部 105 を図 4 に示す構成とするものである。なお、伝搬推定部 103 と符号化部 105 以外の構成は、図 1 と同一構

成であるのでその説明は省略する。

ここでは伝搬状態を示すパラメータとして代表的な遅延プロファイルを扱うものとして説明する。この遅延プロファイルは、各バス成分の遅延時間と、パワー、位相などが含まれている。ここでは、バス成分の遅延時間とパワーと
5 を扱った例を示す。

図1中の伝搬推定部103は基準信号が含まれる受信信号を取り出し、伝搬状態の推定を行う。伝搬状態として遅延プロファイルを求める場合、遅延プロファイルは基となる信号と受信した信号との相関で求められることが知られている。この場合、伝搬推定部103は既知信号である基準信号を用いて、そ
10 の信号系列と受信信号系列の相関値を算出することで遅延プロファイルが得られる。

このようにして得られた伝搬情報は符号化部105によってその特徴が抽出される。特徴抽出の例としてベクトル量子化手法を用いるものが考えられる。これは、代表的な遅延プロファイルのテンプレートを量子化ベクトルとして参考
15 照テーブル上に幾つか用意しておく、更に各量子化ベクトルに対応させた暗号鍵を参照テーブル上に格納しておく。符号化部105は、このように用意しておいた参照テーブルから伝搬推定部103が推定した結果と照合し、最も類似性の高い遅延プロファイルのテンプレートに対応する暗号鍵を選択・出力する。

以上、伝搬状態を推定し、暗号鍵へと符号化する方法について説明したが、
20 図4を用いてさらに詳細に説明する。

図4は、伝搬推定部103と符号化部105を示している。これらは図1の各部位に相当する機能を更に詳細に示したものである。図1の説明では、伝搬推定部103は周波数・時間ずれや位相情報など様々な状態を推定するものとしたが、ここでは遅延プロファイルを推定する方法についてのみ説明する。

25 伝搬推定部103は、バッファ401と、基準信号系列格納部402と、コンボルバ403と、バッファ404とからなり、符号化部105は、量子化部405と、変換部406、コードブック407とからなる。バッファ401は、

入力した受信信号を一定長だけ一時保持するものであり、基準信号系列格納部 402は予め定められた基準信号系列を格納、順次出力するものであり、コンボルバ403は一時保持された受信信号と基準信号系列を畳み込み演算して相関値を出力するものであり、バッファ404は算出された相関系列を一時保持するものである。量子化部405はコードブック407に記録された量子化ベクトルの中から、入力されたベクトル列に最も類似したものを検索しコードを出力する。変換部406は、量子化部405が出力するコードに対応する暗号鍵（第1データ）をコードブックから選択し、出力する。

コードブック407は、この中には量子化ベクトルと暗号鍵が格納されている。図5は遅延プロファイルのテンプレートとなる量子化ベクトルと、それに対応する暗号鍵とが格納されたコードブックの例を示している。

次に、伝搬推定部103と符号化部105の動作を説明する。

まず、伝搬推定部103は、基準信号を含む受信信号をバッファ401に保持する。コンボルバ403は、基準信号系列格納部402からの基準信号系列と、バッファ401に保持された受信信号系列とのスライディング相関を演算した結果を相関系列として出力し、それらを順次バッファ404に保持する。バッファ404で保持された相関系列は、基準信号系列と受信信号系列との相関値、則ち遅延プロファイルに相当するデータが格納されている。これらの遅延プロファイル情報は、一連の入力ベクトルとして符号化部105へと送出される。この様にして求められる遅延プロファイル情報の一例を図6に示す。

量子化部405は、バッファ404からの入力ベクトルと、コードブック407の量子化ベクトルに記録されたベクトルとを照合し、類似性の最も高いものを抽出し、その対応コードを出力する。具体的には、入力ベクトルを X_{in} 、コードmの量子化ベクトルを X_{qm} （m：1～M）とすると、

$$d = |X_{in} - X_{qm}|^2 \quad (1)$$

が最小になる X_{qm} を求ることとなる。このようにして求めた量子化ベクト

ルの対応コードmを出力する。

変換部406は遅延プロファイルの対応コードmと、コードブックの暗号鍵テーブルの内容とから対応する暗号鍵を出力する。このような構成で暗号鍵を決定することにより、柔軟な暗号鍵の設定が簡単な回路で実現可能になる。

- 5 このように、本実施の形態2の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、伝搬推定部103は遅延プロファイルを生成して推定値として基準信号との相関関数を求めるとともに、符号化部105は相関関数と暗号鍵が対応付けられたコードブックを用いて伝搬推定部103から入力した推定値に対応した暗号鍵情報を読み出すので、柔軟な暗号鍵の設定が
10 簡単な回路で実現可能になる。また、本実施の形態2の通信装置及び通信システムによれば、伝搬パラメータをベクトル量子化して遅延プロファイルを求めるので、安定した伝搬パラメータの設定を行うことができる。

なお、本実施の形態2においては、符号化部105の遅延プロファイルの符号化方法として量子化ベクトル手法を用いる方法について説明したが、遅延プロファイルのデータ系列を評価式で近似し、それから得られる近似式の係数を利用するなどして符号化する事や、遅延プロファイルを幾つかのブロックに分割して、その大きさや、順番から符号化したり、最大パワーを有するパスの遅延時間とその大きさによって符号化したりするなど様々な方法が考えられる。

(実施の形態3)

- 20 本発明の実施の形態3に係る通信装置700は、図2に示す本発明の実施の形態1に係る通信装置200において、伝搬制御部701を追加し、かつ符号化部205の代わりに符号化部703を有し、変調部211の代わりに変調部704を有し、送信部212の代わりに送信部705を有している。なお、図2と同一構成である部分は同一の符号を付してその説明は省略する。
25 以下に、伝搬制御により安定した通信方法の発明について、図7および図8を用いて説明する。

図7の送受信装置700は、複数のアンテナ素子から構成されるアンテナ2

01、暗号受信部706、暗号送信部707を具備する。暗号受信部706は受信復調部708と、暗号鍵生成部251と、復号化部207とで構成されており、図1の各部位と同じ構成でなっている。暗号送信部707は、基準信号生成部208と、暗号化部209と、切換部210と、送信変調部709とからなっており、基準信号生成部208、暗号化部209、切換部210は図2中の対応する部位と同じである。

送信変調部709は、伝搬制御部701と、変調部704と、送信部705とで構成されている。伝搬制御部701は伝搬推定部203から出力される伝搬情報と、符号化部703が伝搬情報から特徴を抽出した伝搬特徴情報（第1データ）とを入力し、通信相手の端末に対しての伝搬状態が最適になるように制御するよう、変調制御信号と、送信制御信号とを出力するものである。変調部704は伝搬制御部701から出力された変調制御信号と通信情報とを入力し、変調制御信号に基づき位相や出力タイミング、振幅の微調整などを行いながら通信情報を変調し、各アンテナ素子に対応する変調信号を出力するものである。

送信部705は、送信制御信号と変調信号とを入力し、送信制御信号に基づき、周波数や出力タイミングなどを制御しながら変調信号を、各アンテナ素子に対応するR F信号へ変換しアンテナ201へと出力するものである。

以上のように構成された通信装置について、図8の通信手続きを用いながらさらに詳細に説明する。図8において、基地局、端末とともに図7に示す通信装置として説明を行う。なお、ここでは第1の実施の形態からの相違点のみを記述する。

(0) 基地局、端末：初期化

第1の実施の形態と同様な動作を行う。

25 (1) 基地局：第1基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第1基準信号として出力する。具体的には、切換部210は基準信号生成部208で生成される基準信号を選

択し、送信変調部 709 へ出力する。送信変調部 709 では選択された通信情報と、伝搬情報と伝搬特徴情報とを入力し、通信相手である端末への伝搬状態を制御しながら R F 信号を出力しアンテナ 201 から放射する。この伝搬制御については別途詳細に説明する。

- 5 端末は基地局からの信号を待っており、伝搬推定部 203 は受信した受信信号から第 1 基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。この推定値である伝搬情報は、符号化部 703 と伝搬制御部 701 へ送出される。符号化部 703 は、伝搬推定部 203 からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴情報を伝搬制御部 701 へ出力する。同時に、抽出した伝搬特徴情報を用いて暗号鍵への変換を行う。変換された暗号鍵はバッファ部 206 に保持され暗号鍵情報が出力される。この暗号鍵を第 1 鍵として基地局は以降の通信の暗号鍵とする。
- 10

(2) 端末：第 2 基準信号送信

- 端末は、(1) と同様に基地局で行う伝搬推定用の基準信号を第 2 基準信号として出力する。この時、伝搬制御部 701 は(1) で求めた伝搬情報と、伝搬特徴情報とから、通信相手である基地局に対して暗号鍵（第 1 鍵）に対応する伝搬状態になるように変調部 704 と送信部 705 を制御しながら第 2 基準信号を送信する。

- 基地局では、端末からの信号を受信すると第 2 基準信号を検出し、伝搬推定部 203 は受信信号と既知信号である基準信号とから伝搬推定を行う。(1) と同様、伝搬推定部 203 は伝搬情報を出力し、符号化部 703 は伝搬情報から伝搬特徴情報を抽出して出力する。さらに伝搬特徴情報から暗号鍵へと変換され、バッファ部 206 で暗号鍵情報が保持される。この暗号鍵を第 2 鍵として端末は以降の通信の暗号鍵とする。

25 (3) 基地局：暗号送信

基地局は、切換部 210 の状態を、暗号化部 209 から出力される暗号化情報を選択するように切り換える。暗号化部 209 は(2) で得られた第 2 鍵を

用いてセキュリティデータを予め定められた方法で暗号化し、暗号化情報を出力する。暗号化情報は切換部 210 で選択され、選択された通信情報が送信変調部 709 へと出力される。送信変調部 709 では、伝搬制御部 701 が(2)で求めた伝搬情報と、伝搬特徴情報とから、通信相手である端末に対して暗号鍵(第2鍵)に対応する伝搬状態になるように変調部 704 と送信部 705 を制御しながら RF 信号としてアンテナ 201 から暗号化信号を放射する。

端末は、暗号化信号を受信すると受信復調部 708 が受信信号を復調情報へと復調する。復号化部 207 は復調情報と(1)で求めた第1鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

10 (4) 端末：暗号送信

端末は、(3)と同様に第1鍵を用いて暗号化を行い暗号化情報を出力する。送信変調部 709 では、(1)や(3)で求めた伝搬情報と、(1)で選択した暗号鍵に対応する伝搬特徴情報とから、通信相手である基地局に対して暗号鍵(第1鍵)に対応する伝搬状態になるように変調部 704 と送信部 705 を制御しながら RF 信号としてアンテナ 201 から暗号化信号を放射する。基地局は、(3)と同様に(2)で求めた第2鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

第1の実施の形態で示したことと同様、基地局と端末が生成した暗号鍵(第1鍵および第2鍵)は共有鍵として利用が可能である。則ち、(3)や(4)における暗号化・復号化は問題なく処理されることが分かる。

このように、本実施の形態3の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、伝搬制御部 701 は、符号化部 703 にて生成した暗号鍵と同一の暗号鍵が通信相手においても得られるように変調部 704 と送信部 705 を制御して基準信号を送信する際の伝搬環境を制御するので、通信相手が基準信号を送信する際の伝搬環境と通信相手へ基準信号を送信する際の伝搬環境との誤差を小さくすることができて共通の暗号鍵を生成する際の誤差を小さくすることができる。また、本実施の形態3の通信装置及び通

信システムによれば、送信変調部 709 に於いて受信時で求めた伝搬情報と暗号鍵に対応した伝搬状態を示す伝搬特徴情報とから、通信相手となる端末に対しての伝搬状態を、伝搬特徴情報になるよう制御されているため、受信時の伝搬状態と想定された（暗号鍵に対応する）伝搬状態との誤差が小さくなり、通

5 信品質が大幅に向上するといった有利な特長を有する。

また、伝搬状態が変化した場合でも、伝搬制御を行うことで通信の安定性を向上させることが出来る。

また、暗号鍵を選択する際に符号化部 703 が検索したテンプレートの中で、類似したものが複数存在する場合、送信側が明示的に伝搬状態を制御すること
10 で曖昧さを排除する事が出来る。

なお、本実施の形態 3 においては、通信手順で、基準信号を送信する際、第 1 基準信号の送信と第 2 基準信号の送信を行っているが、両者はどちらが先に実施されても本方式に影響を与えるものではないことは明白である。当然、暗号通信の手順も同様で、その順序によって本方式には影響を与えない。

15 本方式では、基準信号の通信を以て暗号鍵の授受を行っており、基準信号以後の暗号化信号については、その暗号鍵と先に授受したそれとが一致していればよい。つまり、（3）や（4）において送信側が受信側に対して伝搬制御を行いながら通信を行っているが、暗号鍵がしめす伝搬状態と一致する必要はない。

20 また、通信手順の中で基準信号を別途通信しているが、データストリームの中に基準信号を挿入することで、（1）と（3）あるいは（2）と（4）の手順を同時に実施することができるといった有利な特長を有することが出来る。

（実施の形態 4）

通信相手である端末に対して伝搬状態を制御する方法について図 4、図 9 用
25 いて説明する。また、ここでは通信端末のアンテナ 901 は 4 つのアンテナ素子（AN1～AN4）からなるものとする。

図 4 における動作は、上記実施の形態 2 で記述したことと基本的には同一で

ある。ここでは、相違点のみ説明する。

コンボルバ403は、夫々の受信信号に対して基準信号を用いて遅延プロファイルを生成し、4種類の遅延プロファイルがバッファ404で保持される。

ここで、各遅延プロファイルをDs1～Ds4とする。さらに、受信信号と受

5 信重み付け係数(Wr1～Wr4)を用いて、

$$R_0 = \sum R_m \cdot W_r m \quad (2)$$

で与えられる受信信号R0の遅延プロファイル(Ds0)を計算し出力する。

これらの遅延プロファイル(Ds0～Ds4)のうち、Ds0は符号化部105へ入力され、暗号鍵K0、対応コードm0が出力される。

10 なお、受信重み付け係数Wr1～Wr4は初期状態などにおいて初期値に設定されるものとする。

このようにして求められたDs1～Ds4、Wr1～Wr4、Ds0、m0を用いて伝搬制御を行う具体的な方法について図9を用いて説明する。

15 図9のアンテナ901は4つのアンテナ素子で構成され、受信復調部902は各アンテナ素子からのRF信号を入力し、各受信信号および受信系列に対応する受信重み付け係数を出力し、伝搬推定部103は受信重み付け係数と各受信信号とを入力し、伝搬推定を行い伝搬情報を出力し、符号化部105は伝搬情報から特徴を抽出し暗号鍵の対応コードを出力し、伝搬制御部909は伝搬情報と暗号鍵の対応コードと、受信重み付け係数とを入力し、送信重み付け係
20 数を出力し、送信変調部910は通信情報と送信重み付け係数とから各アンテナに対して送信信号を生成し出力するものである。伝搬制御部909は、係数算出部903と、コードブック905と、バッファ904とからなる。係数算出部903は伝搬情報と暗号鍵の対応コード、受信重み付け係数、量子化ベクトルを入力して送信信号のアンテナ素子に対応する送信重み付け係数を出力
25 する。

バッファ904は送信重み付け係数を保持するものであり、コードブック905は対応コードと量子化ベクトルを格納したものである。送信変調部910

は、変調部 906 と、重み付け部 907 と、送信部 908 とからなる。変調部 906 は通信情報を入力して所定の変調方式で変調し、変調信号を出力し、重み付け部 907 は変調信号とアンテナ素子に対応した重み付け係数とを乗じて、重み付け変調信号を出力し、送信部 908 はアンテナ素子に対応する重み付け変調信号を入力し、夫々の信号をアンテナ素子に対応する R F 信号を出力するものである。

次に、受信装置 1000 について、図 10 を用いて説明する。

特徴抽出部 1001 は、受信信号から得られた伝搬情報を入力しその特徴を抽出する。

10 バッファ 1002 は、抽出した特徴抽出情報を一時記憶しておく。そして、バッファ 1002 は、記憶した特徴抽出情報を第 1 データとして出力する。

図 9 で説明した各ブロックの機能は、図 4、図 7 に記述された各部位とほぼ同等である。ここでは、相違点のみについて説明する。

15 アンテナ 901 は 4 つのアンテナ素子 (AN 1 ~ AN 4) から構成されるアンテナであり、受信した R F 信号をアンテナ素子毎の 4 系統出力する。また受信時に用いるアンテナ毎の受信重み付け係数 (Wr 1 ~ Wr 4) も同時に output する。AN 1 ~ AN 4 に対応する受信信号 (R 1 ~ R 4) は伝搬推定部 103 に入力される。上述の通り、伝搬推定部 103 では各受信信号 (R 1 ~ R 4) に対応する伝搬状態 (Ds 1 ~ Ds 4) を出力し、符号化部 105 は暗号鍵 K
20 0、対応コード m0 を出力する。

係数算出部 903 は、暗号鍵 K 0 に対応するコード m0 をコードブック 905 で検索し、コード m0 の対象となっている量子化ベクトル (Xq m0) を読み、保持する。量子化ベクトル (Xq m0) と入力された伝搬情報 (Ds 0 ~ Ds 4) とを用いて、

$$25 \quad d = | Wm \cdot Ds m - Xq m0 |^2 \quad (3)$$

で与えられる 2 乗誤差が最小になるような Wm (m : 1 ~ 4) を求める。この算出法としては最小 2 乗法などが有名である。

こうして得られた重み付け係数 ($W_1 \sim W_4$) と受信重み付け係数 ($W_{r1} \sim W_{r4}$) を用いて、

$$W_{tm} = W_m / W_{rm} \quad (m : 1 \sim 4) \quad (4)$$

で与えられる送信重み付け係数 ($W_{t1} \sim W_{t4}$) を求め出力する。バッファ

5 904 は送信重み付け係数を保持する。

一方、通信情報を入力した変調部 906 は、所定の変調方式に従って通信情報

を変調し、変調信号を出力する。この変調信号は、アンテナ素子 (AN1 ~

AN4) に対応する変調信号系統 (S1 ~ S4) に分岐され、重み付け部 907

へ送出される。重み付け部 907 では、バッファ 904 からの送信重み付け

10 係数 ($W_{t1} \sim W_{t4}$) と、AN1 ~ 4 に対応した変調信号 (S1 ~ S4) を

乗じる。

$$S_{wm} = W_{tm} \cdot S_m \quad (m : 1 \sim 4) \quad (5)$$

こうして得られた重み付け変調信号 ($S_{w1} \sim S_{w4}$) を出力する。送信部

908 は、重み付け変調信号を入力し夫々を RF 信号 ($S_{rf1} \sim S_{rf4}$)

15 に変換してアンテナ 901 へ出力する。

以上のような計算を行いながら送信変調部 910 において送信重み付け係

数を乗ずることで、受信する端末において X_{qm0} で表される伝搬特性の制御

が可能となる。

次に、アンテナ 901 から送信された送信信号を受信した受信装置 1000

20 は、伝搬推定部 103 にて受信信号より伝搬状態を推定して、推定した伝搬状

態情報を特徴抽出部 1001 へ出力する。特徴抽出部 1001 は、伝搬状態情

報より伝搬状態に応じた特徴を抽出して第 1 データとして出力する。

このように、本実施の形態 4 の通信装置及び通信システムによれば、上記実

施の形態 1 の効果に加えて、送受信装置 900 と受信装置 1000 とで同一の

25 第 1 データを取得することができるよう、送受信装置 900 は伝搬推定部 1

03 にて推定した伝搬環境に基づいて通信情報を送信する際の重み付けを調

整するので、ノイズ等が伝搬環境を推定する際に影響することにより送受信裝

置 900 と受信装置 1000 とで同一の第 1 データが取得できなくなるという状態を防ぐことができるとともに、第 1 データの曖昧さをなくすることができます。また、本実施の形態 4 の通信装置及び通信システムによれば、送受信装置 900 は、伝搬推定部 103 にて推定した伝搬環境に基づいて通信情報を送信する際の重み付けを変えることにより、意図的に受信装置 1000 が取得する第 1 データを変更することができるので、長期間同一の第 1 データを使うことにより秘匿情報が解読される等の弊害を防ぐことができる。これにより、第 1 データが暗号鍵である場合には暗号鍵を変更することができるため、高いセキュリティを確保することができる。

10 なお、本実施の形態 4 においては、遅延プロファイルを制御するものとして説明したが、これに限らず、偏波状態（偏波面、旋回方向）や、位相状態、伝搬遅延時間用いて伝搬推定するようにしても良い。また、本実施の形態 4 においては、コードブック 905 は符号化部 105 が持っているコードブックと同一のものであり、構成上はどちらか一方が在ればよい。また、本実施の形態 15 4 においては、アンテナ 901 はアンテナ素子数が 4 の場合について説明したが、これに限らず、2 以上であれば同様の効果が得られることはいうまでもない。また、数式で示した各符号は自然数であっても複素数であっても適用可能である。各値が複素数である場合、信号制御が振幅と位相で行えるため、より高度な制御を期待できる。

20 (実施の形態 5)

本発明の実施の形態 5 に係る通信装置は、伝搬制御を行うことで、任意の暗号鍵を選択できるものであり、図 11 は、本発明に関する通信手順を示したものである。なお、本実施の形態 5 における通信装置は、図 7 に記載した通信装置 700 と同一構成であるので、その説明は省略する。

25 上記実施の形態 1 ~ 4 では、推定した伝搬状態に対応する暗号鍵を選択して通信を行うことから、伝搬状態が一定である場合、暗号鍵が長時間の間同一となってしまう。そのため、暗号鍵の推定が容易になってしまい虞がある。また、

両通信装置で同一の暗号鍵を用いるため、一方の暗号鍵が判明した場合、他方の暗号鍵も判明してしまうといった虞がある。本実施の形態5においては、上記実施の形態1～3においては、第1鍵と第2鍵が同一であったものに対して、これを送信者が選択できるところが異なる。

- 5 図11は、本発明に関する通信手順を示したものである。なお、(0)～(4)の手順は図8と同一であるのでその説明は省略する。

(5) 基地局：第3基準信号送信

基地局は、暗号鍵として第3鍵を選択しその暗号鍵に対応する伝搬特徴情報と、最後に推定された通信の伝搬情報とから重み付け係数を決定する。次に、
10 伝搬制御部701（第2データ選択手段）は、端末で行う伝搬推定用の基準信号を重み付け係数によって伝搬制御を行いながら第3基準信号として出力する。

端末は基地局からの信号を待っており、伝搬推定部203は受信した受信信号から第3基準信号を検出し、受信信号と既知信号である基準信号とから伝搬
15 推定を行う。この推定値である伝搬情報は、符号化部703と伝搬制御部701へ送出される。符号化部703は、伝搬推定部203からの伝搬情報を入力し、伝搬状態の特徴抽出をおこない伝搬特徴情報を伝搬制御部701へ出力する。同時に、抽出した伝搬特徴情報を用いて暗号鍵への変換を行う。変換された暗号鍵はバッファ206に保持され暗号鍵情報が出力される。この暗号鍵を
20 第3鍵として基地局は以降の通信の暗号鍵とする。

(6) 端末：第4基準信号送信

端末は、(5)と同様に暗号鍵として第4鍵を選択しその暗号鍵に対応する伝搬特徴情報と、最後に推定された通信の伝搬情報とから重み付け係数を決定する。次に、基地局で行う伝搬推定用の基準信号を重み付け係数によって伝搬
25 制御を行いながら第4基準信号として出力する。

基地局では、端末からの信号を受信すると第4基準信号を検出し、伝搬推定部203は受信信号と既知信号である基準信号とから伝搬推定を行う。(5)

と同様、伝搬推定部 203 は伝搬情報を出し、符号化部 703 は伝搬情報から伝搬特徴情報を抽出して出力する。さらに伝搬特徴情報を暗号鍵へと変換され、バッファ部 206 で暗号鍵情報が保持される。この暗号鍵を第 4 鍵として端末は以降の通信の暗号鍵とする。

5 (7) 基地局：暗号送信

基地局は、(5)で選択した第 3 鍵を用いてセキュリティデータを予め定められた方法で暗号化し、暗号化信号を送信する。

端末は、暗号化信号を受信すると受信復調部 708 が受信信号を復調情報へと復調する。復号化部 207 は復調情報と(5)で求めた第 3 鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

(8) 端末：暗号送信

端末は、(6)で選択した第 4 鍵を用いてセキュリティデータを暗号化し、暗号化信号を送信する。

基地局は、(7)と同様に(6)で求めた第 4 鍵を用い、予め定められた方法によって暗号の復号化を行い、セキュリティデータを出力する。

以上の動作について数式を交えて説明する。

電波伝搬の特性を表す伝搬関数 H 、受信信号 S_r 送信信号 S_t を用いて表すと、

$$S_r = H \cdot S_t \quad (6)$$

20 の式が成り立つ。アンテナの素子数を N とすると、 H は $N \times N$ の正方行列、 S_r と S_t は $1 \times N$ の行列である。端末は基地局が送信する信号（図 3 では第 1 基準信号）、基地局は端末が送信する信号（図 3 では第 2 基準信号）を用いて計算することができる。第 1 基準信号および第 2 基準信号の通信を式で表すと、

$$S_{r_b} = H_u \cdot S_{t_m} \quad (7)$$

$$25 S_{r_m} = H_d \cdot S_{t_b} \quad (8)$$

と表現できる。 H_u および H_d はアップリンク・ダウンリンクの伝搬関数、 S_{t_b} 、 S_{r_b} は基地局側の送受信信号、 S_{t_m} 、 S_{r_m} は端末側の送

受信信号である。また、 S_t_b および S_t_m は既知信号（第 1、第 2 基準信号）であるから、伝搬関数はそれぞれ、

$$H_u = S_r_b \cdot S_t_m^{-1} \quad (9)$$

$$H_d = S_r_m \cdot S_t_m^{-1} \quad (10)$$

5 で求められる。伝搬関数は伝搬の相反性から、送信時と受信時では同一となることから、

$$H \equiv H_u = H_d \quad (11)$$

である。この様にして得られた伝搬関数 H を暗号鍵（第 1 鍵（＝第 2））に用いるのが第 1 の実施の形態に示したものである。

10 一方、送信重み付け係数 W_b 、 W_m を用いて伝搬状態を制御する方法について説明する。暗号鍵（第 1 鍵（＝第 2 鍵））を選択する際に求めた量子化ベクトルで示される伝搬関数 H' と実際の伝搬関数 H との間に誤差 ε が在る場合は、

$$S_r = (H' + \varepsilon) \cdot S_t \quad (12)$$

で示されるから、誤差成分 ε は、

$$15 \quad \varepsilon = H^{-1} \cdot (S_r \cdot S_t^{-1}) \quad (13)$$

で求めることができる。これを重み付け係数 W_m 、 W_b に置き換えることで、

$$S_r_b = (H' \cdot W_m) \cdot S_t_m \quad (14)$$

$$S_r_m = (H' \cdot W_b) \cdot S_t_b \quad (15)$$

のように補正が可能である。この様にして重み付け係数を用いて伝搬状態を補

20 正しながら暗号通信を行うのが第 4 の実施の形態に示したものである。さて、この補正機能をさらに発展することで、暗号鍵を送信側で設定することも可能である。第 1 鍵（＝第 2 鍵）とは異なる第 3 鍵、第 4 鍵を用いる場合について説明する。基地局は、第 3 鍵に対応する伝搬関数 H_3 になるよう重み付け係数 W_{3_b} によって制御を行い、これを第 3 基準信号を通じて送信する。すなわ

25 ち、

$$S_r_m = (H \cdot W_{3_b}) \cdot S_t_b \quad (16)$$

とした場合、

$$H_3 = H \cdot W_3 _ b \quad (17)$$

である。以降基地局は第3鍵を用いて暗号化を行いながら暗号化通信を実施する。

端末は、第3基準信号を受信し伝搬状態を解析することで、伝搬関数 H_3 を得ることが出来るからそれに対応する暗号鍵（第3鍵）を用いて、以降の暗号化情報を復号していけばよい。同様にして、端末側は第4鍵を選択（対応する伝搬関数は H_4 とする）し、重み付け係数 $W_4 _ m$ によって制御を行いながら第4基準信号を通じて送信する。

$$S_r _ b = (H \cdot W_4 _ m) \cdot S_t _ m \quad (18)$$

$$10 \quad H_4 = H \cdot W_4 _ m \quad (19)$$

端末は第4鍵を用いて暗号化を行いながら暗号化通信を実施する。同様にして基地局が第4鍵を用いて復号可能である。

このように、本実施の形態5の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、伝搬制御部701は基準信号を送信する際に伝搬環境が変化するように送信部705と変調部704を制御するので、任意のタイミングにて暗号鍵を変更することができるので、第三者により暗号鍵を解読される可能性がなくなり、高いセキュリティを提供することができる。

(実施の形態6)

上記実施の形態1～5において説明したフレーム構成は、図12(a)を基準に説明している。つまり、基準信号を含むバーストと、暗号化信号を含むバーストが別に存在している形態である。この方式を用いると基準信号期間を長く取れるため、受信側の推定誤差を小さくできるといった特長がある。

図12(b)の場合は、フレーム構成がデータストリーム（或いはバースト）中に所定の期間、基準信号を挿入する方法である。この方式によると、暗号化信号と同時に暗号鍵を授受することが可能であり、効率的な伝送を行うことが出来るようになる。

一方、図12(c)は、基準信号が示す暗号鍵と暗号化信号が用いる暗号鍵

の配置について示している。図 12 (c) に示すように、基準信号が示す暗号鍵と対応するデータ信号との間で時間的（或いは周波数的）に所定の方式に従って変化を付けることで、暗号鍵と対応する暗号化信号とを独立して授受することが可能となるため、第 3 者へ両者が漏洩する危険性が減るといった特長を有する。

暗号鍵の授受については、他の実施の形態において通信手順にも示した通り、基準信号を用いて行われていることとしている。図 11 の (1)、(2) がそれに相当する。図 11 では、これ以外の通信では暗号鍵の授受は行われていない。これは、暗号化通信時の伝搬状況には復号動作が左右されないことを示している。つまり、基準信号の送信時は伝搬環境に応じて特徴的な伝搬情報が伝達できるように伝搬制御を行うことで安定した暗号鍵の授受が可能となる。

次に、通信手順と対応する伝搬制御の操作を、図 13 を用いて説明する。

まず、図 12 (a) のフレーム構成における通信について説明する。

図 13 の (1 a) において基準信号が送信される際、伝搬制御は他の実施の形態で述べたように暗号鍵を授受するための通信を行う。この時、以前に伝搬推定を実施していれば、その推定結果と暗号鍵に対応する伝搬状態との差を補正するような制御を行うことが可能である。こうすることで受信側は伝搬状態が良好な状態で基準信号を受信可能であり、安定した暗号鍵授受が行えることになる。一方、図 13 の (2 a) において、データ通信（暗号化信号）を行う場合、暗号鍵は既に受信側に届いており、受信・復号に伝搬情報を用いる必要はない。このため、制御方式としては受信が安定して行えるような制御（ピームフォーミング、送信側の等化、送信ダイバーシチなどが知られている）を行うことでデータ通信を安定して行うことが出来る。以降、図 13 の (3 a) 以降の様に通信を行うことで大幅な通信品質の向上が見込める。

次に、図 12 のフレーム構成 (b) における通信について説明する。

図 13 の (1 b) に示すように、基準信号通信時とデータ通信時とで伝搬制御方式を切り換えることが考えられる。この方式を用いると、暗号鍵と暗号化

信号とを同時に伝達することが可能である。送信側で暗号を選択できることは既述の通りであるが、その特性を利用することで毎ブロック暗号鍵を変更するといった柔軟な事も可能になる。その上、先に説明したように安定した通信が行えるといった特長がある。

- 5 一方、基準信号通信時とデータ通信時の伝搬制御方式を同一にすることも当然可能である。この場合、データ通信時の復調に基準信号を利用する事が可能となり、通信品質の向上が見込める。

以上、説明の中で基準信号として既知信号を想定して説明を行った。しかし、基準信号は既知信号である必要はない。この場合、復調しながら伝搬の変化を
10 推定し、暗号鍵を決定する事になる。このようにする事で、暗号鍵を決定するための情報が増加し、安定して暗号鍵の検出が行えるようになる。また、基準信号はQAM変調などに用いられるパイロット信号、TDMAなどで行うバースト同期用の同期信号系列などを用いる事も可能であり、このような構成によると、従来構成をほとんど変更せずに高いセキュリティ性を確保した通信が
15 提供できるといった特長がある。

図12のフレーム構成（b）、（c）のように、データストリームの中に基準信号を挿入することで、図11の（1）と（3）あるいは図11の（2）と（4）の手順を同時に実施することができるといった有利な特長を有することが出来る。

20 以上の説明では、データ通信時の伝搬制御方式をビームフォーミングやプリコーディング（送信側の等化）、送信ダイバーシチなどとしたが、MIMO（Multi-Input Multi-Output）の制御や、空間多重制御（Space Division Multiplexing）などを行うことも考えられる。特にMIMO多重化技術や空間多重技術は、伝搬特性を積極的に利用してチャネル容量の拡大を図る技術であり、本発明に記述されている技術も伝搬特性を積極的に利用したものであり整合性が良い。例えば、上記実施の形態で示した技術を用いて秘匿通信を行った後、伝搬制御をMIMO向け

に（或いは空間多重制御向けに）変更することで引き続き、MIMOや空間多重を行うことが可能となる。この様にすることで、特別な技術構成を追加することなく、重要な情報に対しては秘匿性を高くし、データ通信に対してはチャネル容量を向上させることが可能になる。

5 このように、本実施の形態6の通信装置及び通信システムによれば、上記実施の形態1～5の効果に加えて、通信相手が伝搬環境に基づいて暗号鍵（第1データ）を取得するために送信する信号とそれ以外の信号との送信の際の伝搬環境を変化させてるので、通信相手に暗号鍵を取得させるために送信する信号以外の信号を通信環境に応じて最適な制御方式にて送信することができる。

10 なお、本実施の形態6においては、説明の中で基準信号として既知信号を想定して説明を行った。しかし、基準信号は既知信号である必要はない。この場合、復調しながら伝搬の変化を推定し、暗号鍵を決定する事になる。このよう にする事で、暗号鍵を決定するための情報が増加し、安定して暗号鍵の検出が行えるようになる。また、基準信号はQAM変調などに用いられるパイロット
15 信号、TDMAなどで行うバースト同期用の同期信号系列などを用いることも可能であり、このような構成によると、従来構成をほとんど変更せずに高いセキュリティ性を確保した通信が提供できるといった特長がある。

（実施の形態7）

本発明の実施の形態7に係る通信装置は、図14は、本実施の形態7に係る
20 通信装置における受信装置の一部を示すものであり、図15は、本実施の形態7に係る通信装置における送信装置の一部を示すものである。なお、上記実施の形態1における通信装置と同一構成である部分は同一の符号を付して、その説明は省略する。

ここでは、多重した信号への適用方法について説明する。多重アクセス方式
25 としてはCDMAを例に挙げる。

受信復調部150は、RF信号を受信した受信信号と復調した復調情報とを出力する。受信復調部150は受信部1401、逆拡散部1402、伝搬推定

部 1405、復調部 1403 とからなる。

図 14 は本発明に供する受信装置の一部を示したものである。

受信部 1401 は、R F 信号と伝搬情報を入力し、R F 信号を適切な受信状態に制御し、受信信号を出力し、逆拡散部 1402 は受信信号とチャネルに対応する拡散符号との畳み込み積分を行い逆拡散信号を出力し、復調部 1403 は、受信信号と伝搬情報とから適切な復調を行い復調情報を出力し、復号化部 1404 は、暗号鍵情報と復調情報を入力し、暗号鍵情報から復調情報の暗号を復号化しセキュリティデータを出力し、伝搬推定部 1405 は各チャネルの伝搬推定をおこない各チャネルに対しての伝搬情報を出力し、復調部 1403 は、受信信号と伝搬情報とから適切な復調を行い復調情報を出力し、比較部 1406 はチャネル毎の伝搬情報を比較し比較結果（第 1 データ）を出力し、暗号鍵生成部 1407 は、伝搬情報を入力し暗号鍵情報（第 1 データ）を出力する。

図 15 は本発明に供する送信装置の一部を示したものである。

データ供給部 1501、1502 はチャネル毎のデータを保持し、変調拡散部 1503、1504 はチャネル毎のデータを変調しチャネルに対応する拡散符号で拡散して、拡散信号を出力し、重み付け部 1505 は送信信号と送信重み付け係数を乗じ、送信部 1506 は、変調信号を送信する R F 信号に変換して出力し、アンテナ 1507 は、送信信号を送信し、データ供給部 1508 は第 1 データを格納し、基準伝搬バッファ 1509 は伝搬状態の基準情報を保持し、伝搬制御部 1510 は暗号鍵と第 2 データと伝搬情報を入力し送信重み付け係数を算出する。

次に、送信装置 1500 の動作について説明する。

送信装置 1500 は、データ供給部 1501、1502 から複数チャネル分のデータを取りだし夫々を変調し、予め設定されている拡散符号を用いて各チャネルの拡散信号を生成する。データ供給部 1508 は第 1 データを出力し、

それを入力した伝搬制御部 1510 は、事前に推定された伝搬情報が保持された基準伝搬バッファ 1509 からの情報を基に、第 1 データに対応する伝搬状態制御を、送信重み付け係数によって行う。送信重み付け係数は重み付け部 1505 で重み付け演算が行われ、送信部 1506 を通じて送信される。

5 まず、簡単のためデータ供給部 1508 からの出力がないものとする。伝搬制御部 1510 の制御自体は図 7 で示した伝搬制御部 701 と同一である。例えば、チャネルが 1 つである場合は実施の形態 4 でしめした基準信号を出力している状態と一致する。チャネルが複数ある場合を考える。拡散符号はチャネル毎に設定されているが、各符号間の相関はないため、信号処理上ではそれぞ
10 れが独立に処理されていることと同義となる。則ち、伝搬制御部 1510 はチャネル数を M、アンテナ数を N とすると $M \times N$ 個以上の送信重み付け係数によってチャネル毎に伝搬制御が行えることになる。

以上説明した通り、上記実施の形態 5 同様に暗号鍵に応じた伝搬制御が行えることが分かる。

15 さて、複数チャネルが多重されている場合、チャネル毎に伝搬制御を行うことにより、受信端での受信電力を制御することも可能である。例えば、暗号鍵の状態に応じて、どのチャネルが最大電力とするかを制御できることになり、このチャネル番号と受信電力の関係によって受信装置は暗号鍵を決定することが可能となる。さらに、上述のとおり、伝搬パラメータとして（例えば遅延
20 プロファイル）を設定できるので、例えば遅延プロファイルに暗号鍵情報を、チャネルと受信電力の関係に第 1 データを利用すること（或いは逆でも構わないし、暗号鍵情報だけ、第 2 データだけといったことも可能である）によって、より多くのセキュアな情報を送信することが可能であることがわかる。

さらに、データ供給部 1501、1502 に格納されたデータのうち、1 つ
25 を基準信号とすることも可能である。この様にすることで、受信装置は第 1 データや第 2 データと同時刻に基準信号による伝搬推定の実施が可能になるので、非常に効率の高い传送が可能になるといった特長を有する。

次に、受信装置の動作について説明する。

伝搬パラメータ（遅延プロファイルなど）を用いて暗号鍵情報を授受する方法については、逆拡散処理を除き上述のものと同一に行うことが可能である。ここでは、多重化されたチャネルと受信電力の関係に情報が重畳されている場合についてのみ説明を行う。

アンテナ 101 から入力された R F 信号は受信部 1401 で受信され受信信号が出力される。受信信号は逆拡散部 1402 において、チャネル毎に予め設定された拡散符号とで畳み込み演算が施され、逆拡散信号がチャネル数分出力される。これら逆拡散信号は、伝搬推定部 1405 へ入力され伝搬状態が推定される。ここでは伝搬状態のうち、受信電力を用いるものとする。伝搬推定部 1405 からチャネル毎の受信電力が出力されると、比較部 1406 によって受信電力の比較が行われ、この結果を暗号鍵情報（或いは第 1 データ）として出力する。

この様にして決定された暗号鍵を用いて、復号化部 1404 は以降の復調情報 15 報を復号化し、セキュリティデータを得る。

このように、本実施の形態 7 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、比較部 1406 は、多重された受信信号において、各チャネルの信号の受信電力等の伝搬パラメータの比較結果を情報として送ることができるので、多重信号を送信する場合における情報量を増やすことができる。また、本実施の形態 7 の通信装置及び通信システムによれば、複数チャネルを多重する場合、チャネル毎に伝搬制御を行うことにより、受信端での受信電力を制御することも可能であり、例えば、暗号鍵の状態に応じて、どのチャネルが最大電力とするかを制御できることになり、このチャネル番号と受信電力の関係によって受信装置は暗号鍵を決定することが可能になるので、複数チャネルのデータのセキュリティを維持することができる。また、本実施の形態 7 の通信装置及び通信システムによれば、第 1 データにおける遅延プロファイルのような伝搬パラメータに暗号鍵情報を含めるとともに、チャネルと受

信電力との関係を用いて第1データとは異なる情報の第2データとすることができるので、より多くのセキュアな情報を送信することが可能になる。

なお、本実施の形態7において、CDMAを例に挙げたがOFDMでも同様の効果が得られることはいうまでもない。OFDMとなる場合、上記説明におけるチャネルをサブキャリアとし、図14の逆拡散部処理はフーリエ変換処理に、図15の拡散処理は逆フーリエ変換処理に置き換えることで可能である。

(実施の形態8)

図16は、本実施の形態8に係る通信装置の一部の構成を示す図である。なお、通信装置全体の構成は図1と同一構成であるのでその説明は省略する。

10 本実施の形態8は、伝搬情報として受信到来方向情報を利用した方式について説明する。到来方向推定を行う際の構成を、図7の伝搬推定部203の詳細ブロック図を図16に示す。

伝搬推定部203は、バッファ1601、相関行列演算部1602、行列演算部1603、角度スペクトラム演算部1604、バッファ1605で構成されている。

バッファ1601は、入力信号を一時保持し、相関行列演算部1602は入力信号の相関行列を求め、行列演算部1603は計算された相関行列を入力し行列演算（ここでは固有ベクトル）で求めた固有ベクトルを出力し、角度スペクトラム演算部1604は、固有ベクトルを入力して角度スペクトラム演算し20 到来方向推定情報を出力し、バッファ1605は演算結果を一時保持する。

以上の構成は到来方向推定法として知られているMUSIC法を用いている。他に、フーリエ法やCAME法が知られているが、これは行列演算部1603の演算内容によって分類される。

以上の構成において、伝搬推定部203が伝搬情報として到来方向推定を行う際の動作について詳細に説明する。

複数のアンテナ素子から入力された受信信号は、バッファ1601において保持される。保持された受信信号は相関行列演算部1602においてその相関

行列が求められ、次に行列演算部 1603において固有ベクトルが算出される。角度スペクトラム演算部 1604は固有ベクトルから、受信信号到来パターン情報を算出しこれを出力する。この様にして得られた受信信号到来パターン情報はバッファ 1605で保持される。この様にして求められる受信信号の到来方向情報の一例を図 17に示す。図 17では信号の到来方向が2つ存在する場合の推定結果を示している。

この様にして得られた受信信号の到来パターン情報を用いて、図 11に示す手順で説明を行う。なお、本実施の形態 6 の動作において、上記実施の形態 5 と相違する部分についてのみ説明する。

10 (1) 基地局：第1基準信号送信

基地局は、端末の伝搬推定用に第1基準信号を送信する。この時、複数のアンテナ素子によるビームステアリングを行って、放射パターンを変化させながら送信する。

15 端末は、基地局が出力する基準信号を検出すると、伝搬推定部 203は、到来方向推定を行い、基地局が制御する放射方向と、端末における受信信号到来パターン情報との対比データを参照テーブル上に格納する。以上の操作により、基地局と端末との間における放射パターンと受信到来パターンとの参照テーブルができる。

(2) 端末：第2基準信号送信

20 端末は、暗号鍵（第1鍵）を選択し、コードブックからそれに対応する到来方向情報を出力する。この到来方向情報を、参照テーブルに格納されている放射パターンに最も類似しているものを検出し、これに対応する到来パターン情報を出力時の放射パターンとして設定する。次に、基地局の伝搬推定用に第2基準信号を、設定した放射パターンになるよう制御しながら送信する。

25 基地局は、伝搬推定部 203で到来方向推定を行い受信到来パターンを出力する。符号化部 703は受信到来パターンとコードブックから暗号鍵（第2鍵）を選択し、バッファ 206を介して復号化部 207へ出力する。

(3) 基地局：暗号化信号送信

基地局は、(2)で求めた受信到来パターンから、端末の受信状態が良好になるような放射パターンに設定する。次に第2鍵を用いてセキュリティデータを暗号化し、設定した放射パターンになるよう制御しながら暗号化信号を送信
5 する。

端末は、RF信号を受信復調部708で復調し、復号化部207で第1鍵を用いて復号化し、セキュリティデータを出力する。

(4) 端末：暗号化信号送信

端末は、(1)で求めた受信到来パターンから、基地局の受信状態が良好になるような放射パターンに設定する。次に、セキュリティデータを第1鍵で暗号化させながら設定した放射パターンになるように制御しながら暗号化信号を送信する。
10

基地局は、RF信号を受信復調部708で復調し、復号化部207で第2鍵を用いて復号化し、セキュリティデータを出力する。

15 このように、本実施の形態8の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、角度スペクトラム演算部1604は、受信信号の到来方向推定結果を伝搬環境の推定値として用いるので、第3者に到達する受信到来パターンは大きく変化するため、非常に高いセキュリティを確保出来る。

なお、本実施の形態8において、受信到来パターンを用いて暗号鍵情報を作成することとしたが、これに限らず、伝搬情報として遅延プロファイルを用いる方式と組み合わせることで、一層高いセキュリティが期待できるといった特長を有する。また、本実施の形態6において、受信信号の到来方向に情報を重畳することや、到来方向に対して通信の多重化を行うことも可能である。また、通信手順はここで説明したものに限られるものではない事は、他の実施の形態
20 25 で述べたことと同じである。

(実施の形態9)

本実施の形態9においては、偏波を応用したセキュリティ通信方式について

説明する。

図18は、本実施の形態9に係る通信装置である送受信装置1800の構成を示す図である。なお、図18において、図2と同一構成である部分には同一の符号を付してその説明は省略する。

- 5 アンテナ部1812は垂直偏波アンテナ1801と水平偏波アンテナ1802からなり、伝搬推定部203は、位相差検出部1803と電界強度検出部1804と偏波推定部1805からなり、偏波制御部1813は係数算出部1806とコードブック1807とバッファ部1808からなり、送信変調部252は変調部1809と重み付け部1810と送信部1811とからなる。
- 10 垂直偏波アンテナ1801は垂直偏波成分を受信し、水平偏波アンテナ1802は水平偏波成分を受信し、位相差検出部1803は両偏波受信信号から位相差を検出し、電界強度検出部1804は垂直偏波受信信号と水平偏波受信信号とから夫々の電界強度を検出し、偏波推定部1805は位相差と電界強度から偏波状態を推定する。係数算出部1806は伝搬情報とコードブックで示される偏波コードとを入力し垂直偏波送信信号と水平偏波送信信号との位相差制御と電界強度制御を行って送信信号の偏波制御を行う係数を算出し、コードブック1807は、係数と偏波コードとの関係を記憶し、バッファ部1808は、係数算出部1806から入力したデータを一時的に保持して重み付け部1810へ出力する。
- 15 変調部1809は、通信情報を入力して所定の変調方式で変調し、変調信号を出力する。
- 20 重み付け部1810は、変調信号とアンテナ素子に対応した重み付け係数とを乗じて、重み付け変調信号を出力する。
- 25 送信部1811は、アンテナ素子に対応する重み付け変調信号を入力し、夫々の信号をアンテナ素子に対応するR F信号を出力する。

次に、送受信装置1800の動作について説明する。

垂直偏波アンテナ1801と水平偏波アンテナ1802は受信信号の各偏

波成分を選択的に受信し、R F信号を受信復調部 250へ送出する。受信復調部 250は各偏波に対応する受信信号を出力し、これら受信信号は伝搬推定部 203へ入力される。伝搬推定部 203では、位相差検出部 1803と電界強度検出部 1804から出力される受信位相差情報と受信電界強度情報が偏波推定部 1805に入力され、受信信号の偏波情報が出力される。

図 19 に偏波状態の具体例を示す。E vが垂直偏波の電界強度、E hが水平偏波の電界強度、p が旋回方向、θ が長軸角度を表している。

このようにして求められた偏波情報は符号化部 205によって偏波コードに符号化され、暗号鍵が選択される。この偏波コードは偏波制御部 1813に
10 入力される。偏波制御部 1813では、係数算出部 1806がコードブック 1
807から偏波コードに対応する偏波状態を検索し、位相制御や電界強度制御などを行いながら送信重み付け係数を算出し、バッファ部 1808に保持する。
バッファ 1808に保持された送信重み付け係数は、送信変調部 252によつ
て垂直偏波送信信号と水平送信偏波信号とがそれぞれ重み付けされ、R F信号
15 として対応するアンテナ素子から出力される。

以上のような操作を行うことで、例えば垂直偏波、水平偏波であるとか、長軸の角度、偏波間の位相、旋回方向などが暗号鍵として用いることが可能となる。

伝搬状態のなかで、偏波はアンテナに依ってのみ分離されるという特長がある。

20 なお、コードブック 1807の量子化ベクトルの内容としては、偏波状態（偏波面や旋回方向など）に対応するものが格納されているものとする。通信手順については、他の実施の形態で示したものとほぼ同じである。遅延プロファイルの検出、あるいは伝搬制御の箇所が、夫々偏波情報や偏波制御に置き換わるものである。

25 このように、本実施の形態 9 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、偏波推定部 1805は、電界強度と位相差から偏波状態を推定して伝搬環境の推定値とするので、偏波はアンテナに依ってのみ

分離されるという特長があるため、他の受信装置が電波を傍受したとしても、アンテナが対応してなくてはならないことを意味し、高いセキュリティが期待できる。

なお、本実施の形態9においては、伝搬状態として遅延プロファイルや受信

- 5 パワー、到来方向パターンなどと併用することも可能である。

(実施の形態10)

上記実施の形態1～9に記載の方式に加え、受信端末における通信状態を制御し、その制御状態に対して情報を重畳させる方式を用いて、第3者における傍受を原理的に不可能にする方式について説明を行う。

- 10 実施の形態5において、受信側における伝搬状態を任意に制御できることを示したが、この方式を用いることで物理的に秘匿性のある通信が可能になる。このことを簡単に説明する。

上述した実施の形態5の例では、送信信号の重み付け係数によって伝搬状態を制御できることを示した。このことは、受信側に対して任意の受信状態を伝達していることと同義であり、則ち伝搬パラメータを通じて通信が行えることを意味する。

換言すれば、図5に示すようなコードブックの内容（図中では暗号鍵となっているもの）を情報に置き換えることで、伝搬パラメータを通して通信が可能になることを示唆する。

- 20 この方法を用いた通信は、別途説明したとおり通信者間で形成される伝搬環境をベースとした通信であるため、原理的に物理的位置が異なる装置に対しては高い秘匿性を有するといった特長がある。また、逆に伝搬パラメータを利用して、伝搬経路すなわち通信相手の場所を特定していることになり、通信相手の特定や認証にも応用可能である。

- 25 また、従来利用してきた、変調方式（ASM、FSK、PSK、QAMなど）に依らず適用可能であり、この場合純粹にデータ容量の増加が見込める。

さらに、多重化方式（TDMA、FDMA、CDMA、OFDMなど）など

の縦断に依らず適用可能であるといった大きな特長を有する。本方式は、空間の直交性を利用した多重化も可能である。つまり、空間直交性による多重化方式と上記多重化方式を組み合わせることで、従来のチャネル要領を大幅に増加させることが出来るといった効果も期待できる。

5 また、他の実施の形態で示した暗号化、復号化の処理は特にそれを必要としない装置であれば、必須のものではなくそれがなくても動作することは明白である。

また、他の実施の形態で示した手順の中で暗号鍵情報を送信する必要がない際は、伝搬制御を通信に最適に制御（例えばマルチパス成分を除去したり、受
10 信電力が最大になるよう制御したり）することで通信品質の向上が見込める。

さらに、受信時においても受信信号が受信重み付け係数を用いて最適に制御（上記と同様）する事で、同様に通信品質の向上が見込める。

次に、本実施の形態 10 における受信装置の構成について、図 20 を用いて説明する。

15 図 20 は、本実施の形態 10 に係る通信装置である受信装置 2000 の構成を示す図である。なお、図 1 と同一構成である部分には同一の符号をしてその説明は省略する。

伝搬推定部 103 は、受信部 102 から入力した受信信号から伝搬特性を推定し、推定した伝搬情報をデータとして出力する。伝搬推定部 103 から出力
20 される伝搬情報は、復調部 104 から出力されるデータを破棄するか否かの情報等である。

伝搬特性を通信情報として出力するような受信装置の場合、図 20 に示すような構成で実現可能であり送信部は必ずしも必要ではない。この様に構成することで、伝搬情報を第 1 データとして秘匿性の高い情報として用いることが可能となる。この場合、送信装置では、第 1 データに重要な重畠することも考えられる他に、この第 1 データを用いて通信信号を送信した端末の特定に利用することが可能となる。

このように、本実施の形態 10 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、伝搬推定部 103 は、伝搬推定情報をデータとして使用するので、送信する情報量を多くすることができて伝送効率が向上するとともに、秘匿性の高い情報は伝搬情報として送信することができるので、
5 確実なセキュリティを確保することができる。また、本実施の形態 10 の通信装置及び通信システムによれば、秘匿性の高くなない情報は従来の通信方式により送信することができるので、汎用性のある通信装置を提供することができる。

(実施の形態 11)

図 21 は、本実施の形態 11 に係る通信装置である受信装置 2100 の構成
10 を示す図である。なお、図 1 と同一構成である部分には同一の符号を付してその説明は省略する。

符号化部 105 は、伝搬推定部 103 から入力した伝搬推定情報を符号化して第 1 データとして出力する。この推定した伝搬情報を符号化する技術として、ベクトル量子化法などを用いて符号化し、それを伝送情報として出力すること
15 も可能であり、この様にすることで多様なパラメータ入力に対して、簡易で安定した符号出力が可能であるという特長がある。

このように、本実施の形態 11 の通信装置及び通信システムによれば、上記実施の形態 1 及び実施の形態 10 の効果に加えて、符号化部 105 は、伝搬情報を符号化してデータとして取り出すので、通信品質の向上が見込める。

20 (実施の形態 12)

図 22 は、本実施の形態 12 に係る通信装置である受信装置 2200 の構成を示す図である。なお、図 22 において、図 1 と同一構成である部分には同一の符号を付してその説明は省略する。

逆拡散部 2201 は、受信信号とチャネルに対応する拡散符号との畳み込み
25 積分を行って逆拡散信号を出力する。

比較部 2202 は、チャネル毎の伝搬情報を符号化し、符号化した各チャネルの伝搬情報を比較し比較結果を第 1 データとして出力する。

このように、本実施の形態12の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、比較部2202は、複数チャネルのデータを比較し、その比較結果より第1データを取り出すので、秘匿性が高まると同時により多くのデータを伝送出来るといった特長を有する。

- 5 なお、本実施の形態12においては、逆拡散部を設けることによりCDM信号を用いてデータを取り出すこととしたが、これに限らず、直交周波数分割多重処理された信号を受信して各サブキャリアに配置された信号同士を比較することによりデータを取り出すようにしても良い。また、本実施の形態12の通信装置は、時空間分割多重（MIMO）信号等を用いて通信を行う場合にも
10 適用可能である。

（実施の形態13）

- 本実施の形態13において、図23は、受信装置2300を示す図であり、
図24は、送受信装置2400を示す図である。なお、図1の受信装置100
及び図2の送受信装置200と同一構成である部分は同一の符号を付してそ
15 の説明は省略する。

最初に、受信装置2300について説明する。

- 受信復調部150は受信したRF信号を入力し推定した伝搬情報と復調した復調信号を出力する。符号化部105は伝搬情報を入力しその特徴を抽出し
その伝搬特徴符号（第1データ）を出力し、復号化部107は伝搬情報の特徴
20 を示す符号と復調信号とを入力し、伝搬特徴符号に対応するインタリーパタ
ーンを用いて順序の逆変換（デインタリーブ）、ヌル情報の追加（デパンクチ
ャ）、復号化（デコード）し、セキュリティデータ（第2データ）を出力し、
復調信号を入力し伝搬特徴符号に対応するインタリーパターンに基づきデータ順序の逆変換を行うデインタリーバ2301と、デインタリーブ信号を入
25 力し伝搬特徴符号に対応するパンクチャパターンに基づき除去された箇所の
信号に対して（後段のデコーダにとって符号を判断するのに）中立な情報を付
加するデパンクチャ部2302と、デパンクチャ信号を入力し伝搬特徴符号に

対応する畳み込み符号に対応して復号化するデコーダ2303とからなる。

次に、送受信装置2400について説明する。

受信復調部250は受信したRF信号を入力し、伝搬状態を推定した伝搬情報と、復調した復調情報とを出力する。復号化部207は伝搬情報の特徴を示す符号と復調信号とを入力し、伝搬特徴符号に対応するインタリーブパターンを用いて順序の逆変換（デインタリーブ）、マル情報の追加（デパンクチャ）、復号化（デコード）し、データを出力し、復調信号を入力し伝搬特徴符号に対応するインタリーブパターンに基づきデータ順序の逆変換を行うデインタリーバ2401と、デインタリーブ信号を入力し伝搬特徴符号に対応するパンクチャパターンに基づき除去された箇所の信号に対して（後段のデコーダにとつて符号を判断するのに）中立な情報を付加するデパンクチャ部2402と、デパンクチャ信号を入力し伝搬特徴符号に対応する畳み込み符号に対応して復号化するデコーダ部2403とからなる。符号化部205は伝搬情報を入力しその特徴を抽出しその伝搬特徴符号（第1データ）を出力し、伝搬制御部2404は伝搬状態を入力した伝搬特徴符号に近づけるよう制御する送信重み付け係数を出力し、符号化部205はデータを入力するものであり、符号化（エンコード）し、情報の除去（パンクチャ）、順序変換（インタリーブ）した符号化情報を出力し、データを入力し畳み込み符号を出力するエンコーダ2405と、畳み込み符号を入力しその符号の一部を除去したパンクチャ符号を出力するパンクチャ部2406と、パンクチャ符号の順序を所定の順に並べ替え符号化情報を出力するインタリーバ2407とからなる。送信変調部2410は符号化情報を入力し、変調して伝搬制御し送信するRF信号を出力するものであり、符号化情報を入力し所定の変調を施し変調信号を出力する変調部211と、変調信号を入力し重み付け係数を乗ずることで伝搬制御を行う送信ウェイト部2408と、送信ウェイト信号を入力し送信するRF信号を出力する送信部212とからなる。

次に、送受信装置2400の動作について、図25を用いて説明する。ここ

では、送受信装置2400が図25中の基地局と端末であるものとして説明を行う。なお、本実施の形態13において、端末は送受信装置2400の構成である場合に限らず、受信装置2300の構成を有していても良い。

本実施の形態13における送受信装置2400の動作において、図3と同一
5 の動作である部分の説明は省略する。

まず、予め伝搬状態に対応するインタリーブパターンや、パンクチャバター
ン、エンコードパターンを用意しておき、基地局、端末でこの情報を共有して
おく。

次に、端末は基地局が送信する基準信号により伝搬状態を推定し、これに基
10 づく各種パターンを設定する。基地局も同様に端末から送信される基準信号に
より伝搬状態を推定し各種パターンを設定する。この時、設定されるインタリ
ーブパターン、パンクチャバターン、エンコードパターンが基地局、端末と同
一のものが選択されることは前述の通りである。

以上の様にして、両者の符号化パターンが設定されると次に両者の間で通信
15 を開始する。基地局は、符号化パターンに基づきエンコーダ部2405によっ
て畳み込み符号化が行われ、パンクチャ部2406によってパンクチャリング
が行われ、インタリーバ2407によってインタリーピングが行われ、こうし
て得られた符号化情報が送信変調部2410へ送出され、符号化部205が出
20 力する伝搬特徴符号は、伝搬制御部2404に入力され送信重み付け係数が出
力され、送信部212によってRF信号が出力、放射される。送信重み付け係
数の算出については、実施の形態3で示したようなものと同一である。

端末では、基地局からの信号を受信し、これを受信復調部250が受信し、
伝搬推定、復調を行い、伝搬情報と復調信号を出力する。復号化部207では
入力された伝搬特徴符号に基づき、インタリーブパターン、パンクチャバター
ン、エンコードパターンが選択されている。復号化部207は、伝搬特徴符号
25 と、復調信号とを入力し、デインタリーバ2401では対応するインタリーブ
パターンの逆に対応した順序逆変換（デインタリーピング）を行い、デインタ

リープ信号を出力する。デインターリープ信号はデパンクチャ部 2402 に入力されパンクチャパターンに対応する箇所にヌル信号（後段にあるデコードの際、判断に中立な値）を挿入（デパンクチャリング）したデパンクチャ信号を出力する。デパンクチャ信号はデコーダ部 2403 に入力されエンコードパターンに基づき復号（デコード）を行い、データを出力する。

送信側と受信側において各種符号化パターンを共有していることは前述の通りであり、このため基地局が送信するデータは端末で正常に伝送されることが分かる。

(0) は図 3 と同一の動作である。

10 (1) 基地局：第 1 基準信号送信

基地局は、端末で行う伝搬推定用の基準信号を第 1 基準信号として出力する。端末では、基地局からの信号を待っており、伝搬推定部 203 は受信した受信信号から第 1 基準信号を検出し、受信信号と既知信号である基準信号とから伝搬推定を行う。符号化部 205 は、伝搬推定部 203 からの伝搬情報を入力し、15 伝搬状態の特徴抽出をおこない伝搬特徴符号を出力する。デインターリバ 2401、デパンクチャ部 2402、デコーダ部 2403 はそれぞれ伝搬特徴符号とインターリープパターンのテーブル、パンクチャパターンのテーブル、エンコードパターンのテーブルを持っており、入力された伝搬特徴符号から対応する各種パターン（符号化パターン）を選択する。

20 (2) 端末：第 2 基準信号送信

端末は、(1) と同様に基地局で行う伝搬推定用の基準信号を第 2 基準信号として出力する。

基地局では、端末からの信号を受信すると第 2 基準信号を検出し、伝搬推定部 203 は受信信号と既知信号である基準信号とから伝搬推定を行う。(1)

25 と同様、伝搬推定部 203 が出力する伝搬情報は、符号化部 205 によって伝搬特徴符号へと変換され、復号化部 207 で伝搬特徴符号に対応した符号化パターンが選択される。

(3) 基地局：符号化信号送信

基地局において、符号化部 2409 は (2) で得られた符号化パラメータを用いてデータのエンコード、バンクチャ、インタリープした符号化情報を出力する。符号化情報は送信変調部 2410 へと出力され、それらを変調部 211、
5 送信ウェイト部 2408、送信部 212 を通じて RF 信号が符号化信号として出力される。

端末は、符号化信号を受信すると受信復調部 250 が受信部 202、復調部 204 を通じて RF 信号を復調信号へと復調する。復号化部 207 は復調信号と (1) で求めた符号化パラメータを用い、デインタリープ、デバンクチャ、
10 デコードの順に復号を行い、データを出力する。

(4) 端末：符号化信号送信

端末において、符号化部 2409 は (1) で得られた符号化パラメータを用いてデータのエンコード、バンクチャ、インタリープした符号化情報を出力する。符号化情報は送信変調部 2410 へと出力され、それらを変調部 211、
15 送信ウェイト部 2408、送信部 212 を通じて RF 信号が符号化信号として出力される。

基地局は、符号化信号を受信すると受信復調部 250 が受信部 202、復調部 204 を通じて RF 信号を復調信号へと復調する。復号化部 207 は復調信号と (2) で求めた符号化パラメータを用い、デインタリープ、デバンクチャ、
20 デコードの順に復号を行い、データを出力する。以上のように通信を行うことでデータの授受が行えることが分かる。

このように、本実施の形態 13 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、符号化部 205 は、伝搬環境の推定値よりインタリープパターンやバンクチャパターン等の制御情報を符号化して求め、求めた制御情報を用いてデータを復号化するので、伝搬状態に応じた最適な符号(復号)が可能となるため、通信品質の向上が見込める。また、本実施の形態 13 の通信装置及び通信システムによれば、従来のように符号化パラメータを

通信上でのやりとり（ハンドシェイク）によって授受する必要がなくなり、効率的な上に伝搬環境に素早く対応できるといった大きな特長を持つ。

なお、本実施の形態13において、符号化パラメータを伝搬状態に応じて変化させて通信を行うもの及び送信時に伝搬制御を行うものとして説明を行つたが、これに限らず、他の実施の形態でも示されているとおり、これは必須ではなく、伝搬制御を行わずに送信する等の任意の方法を採用することができる。また、本実施の形態13において、符号化方式として畳み込み符号を用いる旨説明したが、これに限らず、ブロック符号等の任意の符号化方式が採用できる。

また、本実施の形態13において、符号パラメータとしては、エンコードパターン、パンクチャパターン、インタリーブパターンなどを伝搬状態に応じて変化させることとしたが、これに限らず、エンコードパターン、パンクチャパターン、インタリーブパターンの内の一部は固定して用いても良い。こうすることで符号部・復号部をより簡易に構成することが可能である。この場合、通信品質の向上に最も効果的なものを選択することが重要であるが、例えばパンクチャパターンはデータ容量とエラーレートを大きく左右する重要なパラメータの1つであり、このパターンの変更は最も効果的である事が多い。また、本実施の形態9において、図25の(1)と(2)の手順、あるいは(3)と(4)の手順は前後しても構わないことは明白である。

また、基準信号の授受の後に符号化信号の授受を行っているが、例えば基準信号と符号化信号とを同一のフォーマット上に配し、符号化パラメータの選択した後に復号（あるいは符号）を行うような手順としても構わない。この様にデータと符号化パラメータ推定用の基準信号をセットすることで、より細かな符号化パラメータの選択が可能となるといった特長がある。

さらに、以上の説明において伝搬パラメータに応じて最適な符号化パラメータを変化させる方法について示したが、符号化パラメータのみではなく、変調方式自体（QPSK、16QAM）や、CDMAなどの拡散符号長も変化させることができることは明白である。この様にすることで、符号化パラメー

夕同様柔軟性に富み、さらに効率のよい通信が提供できるといった有利な特長を備える。

(実施の形態 14)

上記実施の形態では、主に伝搬状態を用いたデータ通信について説明を行つた。これらは、伝搬状態の推定精度が要求されるといった問題を有している。一般に、推定精度は演算に用いるデータ量に比例するが、データ量が多くなると効率が低下する。また、伝搬推定結果は伝搬推定に用いる基準信号の自己相関にも影響を受ける。これらを解決する手段について、図26を用いて説明する。

図26は、受信装置2600の構成を示す図であり、図27は、伝搬推定部103の構成を示す図である。なお、図1及び図4と同一構成である部分には同一の符号付してその説明を省略する。

最初に、受信装置2600について説明する。

受信部102、伝搬推定部103、等化部2602及び復調部2603は、
受信・復調部2604を構成する。

等化部2602及び復調部2603は、等化復調部2605を構成する。

符号化部2601は、入力された伝搬情報から特長を抽出し、伝搬特長符号(第1データ)を出力する。

等化部2602は、推定された伝搬情報と、その特徴を示す伝搬特徴符号と
を入力し、受信信号から不要成分の除去を行った等化信号を出力する。

復調部2603は、等化信号を入力しそれを復調した結果の復調情報(第2
データ)を出力する。

次に、伝搬推定部103について説明する。

自己相関部2701は基準信号系列を入力しその系列の自己相関関数を出
力し、成分除去部2702は1次遅延プロファイルをと自己相関関数を入力し、
1次遅延プロファイルから自己相関関数成分を除去した2次遅延プロファイル
を出力するものであり、平均化演算部2703は2次遅延プロファイルを入

力し一定期間の推定結果の平均かを施すものである。

次に、受信装置 2600 の動作について説明する。

基本的動作は図 1 と変わらないため、相違点のみ説明する。入力された RF 信号が受信部 102 により出力された受信信号は、伝搬推定部 103 によって
5 伝搬状態が推定される。この情報は、受信部 102、等化復調部 2605、符号化部 2601 へ入力される。符号化部 2601 では入力された伝搬情報から特長を抽出し、伝搬特長符号を出力、この結果が等化復調部 2605 へと入力される。等化部 2602 は推定された伝搬情報と、その特長を示す伝搬特徴符号とを入力し、受信信号から不要成分の除去を行った等化信号を出力する。復
10 調部 2603 は、同様に伝搬情報と伝搬特徴符号とから適した復調手段を用いて等化信号を復調、復調情報を出力する。

この様に、伝搬情報、伝搬特徴符号を等化復調部 2605 に入力し、等化あるいは復調に用いることで、それらを有効に利用して効果的な等化・復調が可能になり、結果として通信品質の向上が見込めるといった特長を有する。

15 とくに、受信信号から不要成分（たとえばマルチバス成分など）を除去する等化部 2602 に、伝搬特徴符号に対応するタップ係数のテーブルを用意しておき、前記符号に対応したタップ係数を用いて等化処理を行うことで、演算量の大幅な削減効果が得られるといった大きな特長がある。その後、伝搬特徴符号と伝搬情報の差分について等化処理を行うことでより簡易な等化処理部の
20 構成が簡単になるといった特長を有する。

次に、伝搬推定部 103 の動作について説明する。

入力された受信信号を一時保持し、これと基準信号系列とがコンボルバ 40 3 によって相関値が演算され 1 次遅延プロファイルが出力される。基準信号系列は、自己相関部 2701 によって自己相関関数が演算されこれが出力される。

25 遅延プロファイルの演算は

$$D_s(t) = \sum (S_r(t+n) \cdot R(n)) \quad (20)$$

ここで、 D_s が推定した遅延プロファイル、 S_r は受信信号、 R は基準信号系

列である。この時、受信信号は送信信号 S_t と伝搬歪 P_d を用いて

$$\begin{aligned} S_r(t) &= \sum (S_t(t-n) \cdot P_d(n)) \\ &= S_t(t) * P_d(t) \end{aligned} \quad (21)$$

(但し、*’は畳み込み演算を示す)

5 で表すことができ、さらに送信信号 S_t は基準信号であることから

$$\begin{aligned} D_s(t) &= \sum ((S_t(t+n) * P_d(t+n)) * R(-n)) \\ &= (R(t) * P_d(t)) * R(t) \\ &= R(t) * P_d(t) * R(t) \end{aligned} \quad (22)$$

となる。ここで

$$10 \quad A_R(t) = R(t) * R(t) \quad (23)$$

を用いると(数22)は

$$D_s(t) = A_R(t) * P_d(t) \quad (24)$$

となることがわかる。

一例として、基準信号に最長線形符号系列(M系列)を用いることを考える。

15 M系列の符号は、(数23)の自己相関関数 $A_R(t)$ が、 $t=0$ ($0 \leq t < 2^n - 1$) の場合 $2^n - 1$ 、その他では -1 であるといった特長を有する
(図28(a))。このため、自己相関関数をインパルスと見なす事が可能で、
周波数特性としてはこれを無視することが可能である。ある条件の下では、図
6に示すような伝搬特性(遅延プロファイル)が求められるが、この周波数特
20 性は則ち伝搬特性とシステム上のフィルタの特性との合成であることになる。
一方、基準信号系列に合成符号の一種であるゴールド符号系列を用いた場合、
M系列の符号とは異なり、自己相関関数 $A_R(t)$ の $t \neq 0$ の部分において一
定とはならない(図28(b))。このような自己相関関数はインパルスではなく、
周波数特性として遅延プロファイル $D_s(t)$ に影響を与えててしまう。
25 図29に、基準信号をゴールド符号に置き換えた場合の推定結果を示すが、自
己相関関数の影響を受け、図6とは波形が異なっていることが分かる。

この様に、(数20)で示された通り、ここで求めた遅延プロファイルには、

基準信号系列の自己相関関数が含まれているため、基準信号系列の特性に影響されてしまうことがわかる。成分除去部 2702 は自己相関部 2701 が算出した自己相関関数 (A R (t)) の成分を一次遅延プロファイルから除去する演算を行う。具体的には、自己相関関数で与えられるインパルス列を IIR フィルタのタップ係数として除去できることが知られている。

さらに、平均化演算部 2703 において、複数回演算した結果（2 次遅延プロファイル）の平均化を施すことによって、歪やノイズにより発生する誤差を抑えることが可能となる。

このように、本実施の形態 14 の通信装置及び通信システムによれば、上記 10 実施の形態 1 の効果に加えて、等化部 2602 は、セキュリティデータを等化処理した後に復調するので、品質の良いセキュリティデータを得ることができる。また、本実施の形態 14 の通信装置及び通信システムによれば、成分除去部 2702 は、基準信号の周波数成分を除去するので、基準信号の周波数成分の影響を受けない精度の良い伝搬環境の推定値を得ることができる。

15 なお、本実施の形態 14 において、図 26 に示す伝搬推定部 103 と図 26 に示す受信復調部 2604 はそれぞれ独立して受信装置に組み込むことが可能であり、他の実施の形態で示した装置に適用可能であることは明白である。特に、これらと一緒に実施することでより大きな効果が期待できるといった特長を有する。

20 (実施の形態 15)

図 30 は、本実施の形態 15 の通信装置に係る伝搬推定部 103 の構成を示した図である。なお、伝搬推定部 103 を適用した通信装置は、図 1 と同一構成であるので、その説明は省略する。

25 バッファ 3001 は遅延プロファイルを一時記憶し、ベクトル量子化部 30 02 は記憶された遅延プロファイルをコードブック 3008 の内容と照合し最も類似したコードを出力し、符号変換部 3003 はベクトル量子化されたコードを入力しこのコードと対応する符号をコードブック 3008 の符号格納

部 3007 から求め符号を出力し、自己相関部 3004 は基準信号系列を入力しその自己相関関数を出力し、畳込演算部 3005 はコードブック 3008 のうち量子化ベクトルの内容に自己相関関数を畳み込むものであり、コードブック 3008 はベクトル量子化の際に参照する量子化ベクトルとそれに対応する符号を格納し、図 5 に示すような構成である。コードブック 3008 は量子化ベクトル格納部 3006 とそれに対応する符号格納部 3007 とからなつており、これらの構成は他の実施の形態と同一である。

次に、伝搬推定部 103 の動作について説明する。

受信信号がバッファ 401 により一時記憶され、この受信信号系列と基準信号系列格納部 402 が出力する基準信号系列とがコンボルバ 403 に入力される。コンボルバ 403 では、基準信号系列と受信信号系列とのスライディング相關演算を行うことで、遅延プロファイルを求める。これら遅延プロファイルはバッファ 401 により一時保存され、ベクトル量子化部 3002 に送られる。一方、基準信号系列格納部 402 から出力された基準信号系列は、自己相関部 3004 によって自己相関が演算されその値が畳込演算部 3005 へと送出される。ベクトル量子化部 3002 は、入力された遅延プロファイルとコードブック 3008 にある量子化ベクトル格納部 3006 の各ベクトルとのメトリクス量を演算し、その値が最小になるようなベクトルを選択するが、その際、自己相関部 3004 によって自己相関関数が畳み込まれたベクトルを用いてメトリクス演算を行う。ベクトル量子化部 3002 はこのようにして選択したベクトルコードを出力する。符号変換部 3003 は、ベクトル量子化部 3002 が出力したベクトルコードと、コードブック 3008 にある符号格納部 3007 から対応する符号を選択し伝搬推定情報を出力する。

このように、本実施の形態 15 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、畳込演算部 3005 は、ベクトル量子化の際に量子化ベクトルに自己相関関数を畳み込むので、高精度なインパルス応答特性を得ることができる。また、本実施の形態 15 の通信装置及び通信システムに

よれば、伝搬推定情報を高精度に求めるといった効果を有する。また、本実施の形態 15 の通信装置及び通信システムによれば、量子化ベクトル格納部 300 6 にあるベクトルに基準信号系列の自己相関関数を畳み込むことで、探索するベクトルに自己相関関数 AR (n) の成分を与えることと等価となり、(数 5 20) で与えられる Ds (t) にある AR (n) に左右されずに探索する事が可能となり、基準信号系列の自己相関関数に左右されない量子化ベクトルの設定が可能となる。また、本実施の形態 11 の通信装置及び通信システムによれば、自己相関関数を量子化ベクトルに自己相関関数の成分を加えるため、畳込演算を行うのみで可能であり、容易に実現が可能になるといった大きな特長を 10 有する。

(実施の形態 16)

図 3 1 は、本実施の形態 16 に係る受信装置 3100 の構成を示す図であり、図 3 2 は、伝搬推定部 103、変換部 3101 及び符号化部 105 の構成を示す図である。なお、図 1 と同一構成の部分には同一の符号を付してその説明は 15 省略する。

変換部 3101 は、遅延プロファイルをフーリエ変換し、フーリエ変換した係数の中で主要な係数を選択して出力する。

次に、伝搬推定部 103、変換部 3101 及び符号化部 105 の構成について、図 3 2 を用いて説明する。図 3 2 は、フーリエ変換手段を加えることで効率的な符号化を可能にする方法について示したものである。

最初に、伝搬推定部 103 について説明する。

バッファ 3201 は、入力した受信信号を一定長だけ一時保持する。

基準信号系列格納部 3202 は、予め定められた基準信号系列を格納、順次出力する。

コンボルバ 3203 は、一時保持された受信信号と基準信号系列を畳み込み演算して相関値を出力する。

バッファ 3204 は、算出された相関系列を一時保持する。

次に、変換部 3101について説明する。

フーリエ変換部 3205は、遅延プロファイルを入力しそれをフーリエ変換等の直交変換する。

係数抽出部 3206は、フーリエ変換した係数を入力し主要な係数のみを選

5 択する。

次に、符号化部 105について説明する。

ベクトル量子化部 3207は、コードブック 3209に記録された量子化ベクトルの中から、入力されたベクトル列に最も類似したものを検索しコードを出力する。

10 符号変換部 3208は、ベクトル量子化部 3207が出力するコードに対応する暗号鍵をコードブック 3209から選択し、出力する。

コードブック 3209は、図5に示すように、量子化ベクトルと暗号鍵が格納されている。

15 図33は、具体的な遅延プロファイルの状態を示したものであり、横軸は時間（図ではサンプルタイミング）、縦軸は信号振幅で示されている。相関値は、受信信号系列の同相成分（I成分）と直交成分（Q成分）の夫々から求めており、図中の実線は I成分の相関係数、破線は Q成分を示している。以下、I成分およびQ成分は複素数の実数部および虚数部として表すこととする。また、一定時間内における最大の瞬時振幅を有する複素信号により正規化してある。

20 図33に、基準信号系列が生成され、遅延プロファイルが得られるまでのプロックダイアグラムを示す。図33に示されるとおり、送信装置 200では、基準信号系列格納部 3301で生成された基準信号系列が、まず帯域制限フィルタ 3302によって出力信号の波形形成が為される。この信号は、送信部 3303によって空間に放射される。放射された電磁波は、様々な反射、回折などで形成される伝搬空間 3304を通じて受信装置 100へと到達する。受信装置 100では、まず受信部 3305で受信された受信信号系列は、帯域制限フィルタ 3306によって、帯域制限されチャネル選択やノイズ成分除去が為

される。受信信号は帯域制限された後、相関部 3308 で基準信号系列格納部 3307 が output する基準信号系列との相関を求め、送信装置 200 が output した基準信号系列を抽出する。以上の事について、数式を用いて説明する。（数 1
7）で与えられる受信信号 $S_r(t)$ には、帯域制限フィルタ 3306 (F_r
5 (t)) が施されている事から、

$$\begin{aligned} S_{r'}(t) &= F_r(t) * S_r(t) \\ &= F_r(t) * (S_t(t) * P_d(t)) \end{aligned} \quad (25)$$

となる。式 25 の送信信号 $S_t(t)$ は基準信号系列に帯域制限フィルタ 30
02 ($F_t(t)$) を通過していることから、
10 $S_{r'}(t) = F_r(t) * ((F_t(t) * R_s(t)) * P_d(t))$

(26)

である。遅延プロファイルを求めるには、前述の通り基準信号系列 $R_s(t)$ との相関系列を畳み込み演算することで得られるから、

$$\begin{aligned} D_s(t) &= S_{r'}(t) * R_s(t) \\ &= F_r(t) * F_t(t) * R_s(t) * R_s(t) * P_d(t) \\ &= F(t) * A R_s(t) * P_d(t) \end{aligned} \quad (27)$$

で与えられることになる。この時、 $F(t)$ を帯域制限フィルタ 3302 と帯域制限フィルタ 3306 との合成特性で示されるインパルス応答であり、このフィルタ特性を帯域制限フィルタと呼ぶことにする。一方、 $A R_s(t)$ は基準信号系列 $R_s(t)$ の自己相関関数を示している。この様にして求められた（式 27）は自己相関関数 $A R_s(t)$ に伝搬特性 $P_d(t)$ を重畳した信号が、帯域制限フィルタによって帯域制限された特性を表している。ここで自己相関関数 $A R_s(t)$ がインパルス特性であるとすると、伝搬特性 $P_d(t)$ に帯域制限フィルタが掛かった特性と等価であることになる。

25 伝搬特性 $P_d(t)$ を周波数特性として考えた場合、 $F(t)$ によって与えられる周波数特性を加えた伝搬特性が $D_s(t)$ として求められる事がわかる。例えば、 $F(t)$ が $-1/2 f_{bw} \sim +1/2 f_{bw}$ の帯域制限フィルタであ

るとした場合、 f_{bw} で帯域制限された伝搬特性 $P_d - bw(t)$ が求められる。室内伝搬などの環境では、伝搬特性の周波数特性は 1 MHz 以上の帯域が主要であることから、シンボルレートが 1 MHz 以上の通信に於いて特に有効であることがわかる。一方、屋外伝搬の場合は、伝搬特性の周波数特性は 10 kHz 以上の帯域が主要であることから、シンボルレートが 10 kHz 以上の通信に於いて有効である。
5 kHz 以上の帯域が主要であることから、シンボルレートが 10 kHz 以上の通信に於いて有効である。

さて、受信信号から求めた伝搬特性 $D_s(t)$ には、 $F(t)$ で与えられる周波数帯域に制限された伝搬特性成分のみが求まるため、 $D_s(t)$ を変換部 3101 のフーリエ変換部 3205 によって周波数ドメイン領域に変換する
10 ことで、パラメータが低域部分に集中する事がわかる。このようにして周波数ドメイン領域に変換した信号系列の内、周波数の低域部分のみを選択・抽出する係数抽出部 3206 によって、伝搬特性の主要な成分を少ないパラメータで表現することが可能となる。具体的には、図 29 に伝搬特性として求められた $D_s(t)$ の波形を示す。この波形をフーリエ変換した信号系列を図 34 に示す。図 34 を見ると分かることおり、約 12 の要素に主要な信号成分が凝縮されていることが分かる。これは、換言すると図 29 で示した 100 サンプル × 2 要素以上の信号系列がおよそ 10 程度の要素で表現が可能であることを示しており、このことから非常に簡易な構成でベクトル量子化が可能になることを意味する。

20 このように、本実施の形態 16 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、変換部 3101 は、伝搬推定値をフーリエ変換して主要な係数のみを抽出するので、伝搬環境を最も如実に数値化することができる。また、本実施の形態 16 の通信装置及び通信システムによれば、ベクトル量子化部 3207 は、変換部 3101 にて伝搬推定値をフーリエ変換して
25 主要な係数のみを抽出した後にベクトル量子化するので、非常に簡易な構成でベクトル量子化が可能になる。また、本実施の形態 16 の通信装置及び通信システムによれば、フーリエ変換して主要な係数のみを選択して符号化するので、

少ない伝搬パラメータで効率よく第1データを取得することができる。また、本実施の形態16の通信装置及び通信システムによれば、変換部3101を伝搬推定部103と符号化部105との間に挿入することで、大幅な簡略化が可能になるといった非常に大きな特長を有する。

5 なお、本実施の形態16においては、変換部3101にてフーリエ変換を用いた、これに限らず、他にもDCT（離散コサイン変換）や、ウェーブレット変換、ヒルベルト変換などに置き換えても同様の効果が得られることが知られている。

(実施の形態17)

10 図35は、本実施の形態17に係る送信装置3500の構成を示す図であり、図36は、本実施の形態17に係る受信装置3600の構成を示す図である。送信装置3500は、送信データを変調信号に加えて、受信端での信号電力に重畠して通信を行う。受信装置3600は、受信信号の受信電力から重畠された情報を検出する。

15 最初に、送信装置3500について説明する。

変調部3501は第1送信データを一時保持しチャネル数分のチャネル変調信号を出力し、拡散符号格納部3502はチャネル数分の拡散符号を格納しそれを出力し、拡散部3503はチャネルデータとチャネルに対応する拡散符号を疊み込み演算し周波数拡散を行い、伝搬制御部3504は第1送信データを入力しチャネル毎にアンテナ係数を算出し、合成部3505は拡散信号にアンテナ係数を乗じ信号合成したアンテナ信号を出力し、送信部3506は重み付け信号を周波数変換し増幅し、アンテナ部3507は対応する系列の信号を放射する。

次に、受信装置3600について説明する。

25 アンテナ部3601は受信RF信号を出力し、受信部3602は受信RF信号を入力し電力増幅や周波数変換を行い、拡散符号格納部3603はチャネル数分の拡散符号を格納しそれを出力し、逆拡散部3604はチャネルに対応す

る拡散符号と受信信号とを畳み込み演算により逆拡散しチャネル信号を出力し、復調部 3605 はチャネル信号を夫々入力して復調しチャネル復調信号を出力し、電力検出部 3606 はチャネル毎の受信電力を検出し受信電力情報を出力し、バッファ 3607 はチャネル復調信号を一時保持し第 2 データを出力し、比較部 3608 は受信電力情報を入力しその大きさを比較して第 1 データを出力する。

次に、送信装置 3500 及び受信装置 3600 の動作について、図 37 を用いて説明する。図 37 は、伝搬情報として得られる受信電力に情報を重畠する通信方法について説明したものである。

10 図 37 では、送信装置を図 35 と同一構成とするとともに受信装置を図 36 と同一構成にするものであるが、便宜上このように説明するだけで両装置とともに送受信可能な端末であってもよい。

(0) 初期化

15 送信装置および受信装置は電源投入後、所定の初期動作を行い各種パラメータなどの値を所定の値に設定する。

(1) 基準信号送信

受信装置は、伝搬状態を検出するための基準信号を出力する。送信装置は、基準信号を検出するとその信号を基に受信装置からの伝搬状態を算出する。

(2) 暗号送信

20 送信装置は、(1)で得られた伝搬状態を用いて、受信端における電力制御に情報を重畠して通信信号を出力する。受信装置は、通信信号を受信した受信信号を復調すると同時に、信号の受信電力を検出しこれに重畠された情報を検波する。以下、同様に手続きを行う。

次に、図 37 の手続きに従って、各部位の動作を詳細に説明する。

25 ここでは、チャネルの数を 3 (チャネル A、チャネル B、チャネル C)、アンテナの数を 4 (アンテナ 1、アンテナ 2、アンテナ 3、アンテナ 4) とする。

また、送信装置では、前述の通信手順 (1) によって受信装置からの伝搬状態

が算出されているものとする。

第1データと第2データを入力すると、変調部3501は第2データを一時保持し、3チャネル数分のチャネル変調信号を出力する。チャネル変調信号は、拡散部3503へと送出され、拡散符号格納部3502から与えられる拡散符号との畳み込み演算により周波数拡散が行われ、チャネル拡散信号が出力される。伝搬制御部3504は、通信手順(1)によって得られた伝搬状態と、入力された第1データとを用いて受信端での電力が所定の状態になるようなアンテナ係数を出力する。

電力に情報を重畠する方法としては、各チャネルの電力の順番に重畠する方法や、チャネル間の電力の差や電力の比に情報を重畠する方法が考えられる。
10 ここでは、電力の順番に情報を重畠する方法について述べる。

例えば、第1データを3チャネルの電力の順番に重畠する場合
チャネルAの電力>チャネルBの電力>チャネルCの電力
チャネルAの電力>チャネルCの電力>チャネルBの電力
15 チャネルBの電力>チャネルAの電力>チャネルCの電力
チャネルBの電力>チャネルCの電力>チャネルAの電力
チャネルCの電力>チャネルAの電力>チャネルBの電力
チャネルCの電力>チャネルBの電力>チャネルAの電力
といった具合に6通りの情報を重畠できる。

20 この6通りのパターンに夫々符号を割り当て、予め送信装置と受信装置で共有しておくものとする。

伝搬制御部3504は、第1データに対応する電力情報に応じて、チャネル変調信号に対するアンテナ係数を求める。

アンテナ係数を用いて電力を制御する方法について、図38を用いて詳細に説明する。図38では、送信装置と受信装置に設けられたアンテナと、送受アンテナ間で決定される伝搬係数および、各アンテナから入出力される信号との関係を表したものである。ここで、A1～4は送信装置に設けられたアンテナ、

A_rは受信装置に設けられたアンテナ、S_{t 1～4}は送信RF信号、S_{rx}は受信RF信号、h_{1～4}は伝搬係数である。また、図中に示した合成部3505は、図35における合成部3505に相当するものであり、チャネル拡散信号S_{c 1～4}とアンテナ係数C_{11～C34}との演算関係を示している。（送
5 信部は省略してある）これらの関係を数式に表すと

$$\begin{aligned} S_{rx}(t) &= \sum S_{tn} \cdot h_n \\ &= \sum (\sum S_{cm} \cdot C_{mn}) \cdot h_n \quad (28) \end{aligned}$$

で与えられる。送信装置は、通信手順(1)の基準信号によって求めたh_{1～4}の値から、C_{11～C34}の値を調整することによりアンテナA_rで受信される受信信号S_{rx}における受信電力をチャネル拡散信号S_{c 1～3}について独立に調整可能である。特に、C_{11～C34}の位相を変化させるだけで制御を行った場合、各アンテナから放射される電力が変化することがないといった特徴がある。

例えばチャネルA(S_{c 1})は、A_{1～4}から放射された信号が空間合成によってA_rにおいて最大電力になるようにC_{11～C14}が算出され、チャネルB(S_{c 2})は同様にしてノッチが形成されるようにC_{21～C24}が算出され、チャネルC(S_{c 3})に関してはチャネルAとチャネルCとの中間の電力になるようにアンテナ係数C_{31～C34}を算出する。

合成部3505では、アンテナ係数とチャネル変調信号とを入力し、アンテナ_{1～4}に対するアンテナ信号が合成される。アンテナ信号は、送信部3506で周波数変換され電力増幅された後、アンテナ部3507で放射される。

この様にして出力された暗号化信号は、受信装置のアンテナ部3601で受信され、その受信RF信号が受信部3602へと送出される。受信部3602では受信RF信号を入力し、それを電力増幅、周波数変換した受信信号を出力する。受信信号は逆拡散部3604に入力され、拡散符号格納部3603から入力される拡散符号との畳み込み演算が行われる。逆拡散はチャネル数分（ここでは3チャネル分）に対して行われ、チャネル毎に分離されたチャネル信号

が出力される。復調部 3605 では、チャネル信号を入力しそれを復調してチャネル復調信号を出力すると共に、電力検出用にチャネル検出信号を出力する。バッファ 3607 では、復調部 3605 から入力したチャネル復調信号を一時保持し、第 1 データとして出力する。電力検出部 3606 はチャネル検出信号 5 を入力し、チャネル毎の受信電力を推定し、チャネル電力情報を出力する。比較部 3608 では、チャネル電力情報で与えられる電力値を比較し、その結果から予めチャネル電力の順番に割り当てられた符号に変換し第 1 データとして出力する。

送信装置 3500 が発した第 1 データは受信装置 3600 で第 1 データとして用いることが可能となり、特に第 2 データは、送信装置 3500 と受信装置 3600 の間で形成される伝搬路を積極的に利用した通信であるため、他の受信装置では受信が出来ないといった特徴を有しており、セキュリティが重要な情報に対して有効な通信手段となることはいうまでもない。

以上の説明に加え、従来技術との差異について図 39～42 を用いて詳細に行う。図 39 は従来技術としての例である。信号 Sc1～3 の出力電力を C1～C3 により制御し、且つ W1～W4 を用いて指向性制御を行う例を示している。図 39 と図 38 では、図 39 が全てのアンテナに対して同一の重み係数 (C1～C3) を乗じている一方、図 38 では Sc1～3 に対してアンテナ毎に重み係数 (C11～C34) を独立して制御するような構成となっている。図 3 20 9 の様に全アンテナに対して同一の重み係数を用いた場合、指向性で与えられた放射特性に対してその大きさの特性が与えられることになる。

図 40～42 は、空間の断面の位置を横軸に、その場所に於ける受信電力を縦軸にして、各信号の電力分布を描いたものであり▲印が、ターゲットとする受信端末の設置場所を示している。図 40 は、図 39 で得られる特性を示して 25 ある。図 40 に示すとおり、全ての信号分布は相似形になっており、分布形状が W1～W4 で与えられる指向性制御の特性を表している。このため、受信位置がターゲットとする位置からずれていても、受信信号電力は相対的に変化し

ない事がわかる。一方、図38によって伝搬制御された信号分布を図41に示す。送信信号は、各アンテナに対して異なる係数の組合せを有するため、（結果として指向特性が異なるため）受信位置によって各信号の受信電力が異なるといった特徴がある。則ち、ターゲットとする受信位置に対しては、制御したとおりの電力比となっている（●印）が、場所が異なると受信電力の比は異なってしまう。この事を利用することで、送信端末がターゲットとする受信位置以外では、受信電力を用いた復調は出来ないことになる。

また、図38の重み係数C11～C34によって、受信電力が0となるヌル点の制御も可能である。このヌル点は出力アンテナの数をnとするとn-1個のヌル点を制御することが可能であることが知られている。ここで、送信信号（例えばS_c1）を指向性制御によって、受信位置において十分な受信電力になるように制御し、一方、その他の送信信号（例えばS_c1、S_c2）を制御可能なヌル点の幾つか（或いは全て）をターゲットとする受信位置になるように制御する。このように、n（n≥2）個のアンテナからm種類（m≥2）以上の信号を伝搬制御して送信し、その信号の伝送制御は受信アンテナに対して適切な電力が供給されるように制御し、一方、伝送する必要のない信号に対して送信制御は受信アンテナに対して最大n-1のヌル制御を行うことが可能である。なお、m種類の信号において、少なくとも1つが伝送するための信号であれば、伝送するための信号の数は2以上であっても良い。図42にこの様に制御された状態を示す。

図42では、破線で示された各信号（S_c2、S_c3）が▲の場所に於いてヌルを形成し、受信電力が低く制御されている一方、実線で示された信号（S_c1）は十分な受信電力が得られている様子が示されている。ここで送信端末は、S_c1に送信すべき情報を、S_c2、S_c3には疑似情報（或いは重要でない情報）を重畠しておくものとする。この様な通信を行うことで、ターゲットとする受信位置における受信信号は、S_c1のみとなるため、受信端末は受信信号をそのまま復調することでS_C1の情報を得ることが可能となる。一方、

その他の場所でこれらの信号を受信しようとすると、受信信号は Sc 1～3 の電力が入っているため、分離することが困難となる。また、仮に分離が可能であつたとしても Sc 1～Sc 3 のどれが受信すべき情報であるかを推定不可能であるため、正しく復調することが出来ない。

- 5 この様にヌル点を制御する方法を用いると、受信時においてそもそも受信すべき情報しか受信しないため、受信端末は従来と同様の構成で構わない。則ち、送信端末のみを変更することでセキュリティが確保された通信を実施することが可能となるといった大きな特長を有する。

このように、本実施の形態 17 の通信装置及び通信システムによれば、上記
10 実施の形態 1 の効果に加えて、送信側の合成部 3505 は、複数のアンテナを用いて異なる伝搬路にて通信相手へ第 1 データを送信し、受信側の比較部 3608 は、異なる伝搬路を経由してきた到来波を受信して各経路の伝搬環境の推定値の比較結果より第 1 データを得るので、第三者の通信装置を用いて第 1 データを傍受することを極めて困難にすることがでて高いセキュリティを確保することができる。また、本実施の形態 17 の通信装置及び通信システムによれば、送信装置 3500 は複数チャネルを周波数拡散したあと、これを多重する際にアンテナ係数を乗じてチャネル毎に伝搬状態を制御することで、伝搬状態（ここでは信号電力、則ち伝搬ロス）に情報を重畳することが可能となる。

また、本実施の形態 17 の通信装置及び通信システムによれば、信号電力に情報を重畳する手法として ASK に代表される振幅変調があるが、伝搬状態を積極的に利用する点、つまり受信アンテナ端における信号電力を用いているため他の受信点では伝搬特性が異なるために正常に受信できない点で大きく異なっている。たとえば、前述の通りアンテナからの出力電力を変化させることなく受信端における信号電力を変化させることが可能なため、第 3 者が送受信の
20 通信を傍受し、これを復調しようとしても第 2 受信データを復調することは不可能であることから高いセキュリティを確保できるといった大きな特長を有する。また、本実施の形態 17 の通信装置及び通信システムによれば、マルチ

キャリア信号を用いキャリア間の信号電力差に着目して通信を行う様にすること、同時に受信した信号から検波が行えるといった大きな特長がある。これは、同一時刻、同一周波数であることから、伝搬条件は同一のものであると見なせるため、安定した通信を提供することが可能になる。例えば、2チャネルを多重した拡散信号を用いる場合（チャネルRとチャネルSとする）、チャネルRを基準として、その信号電力に対してチャネルSの信号電力が大きいか小さいかを符号に割り当てることも考えられる。信号位相に情報を多重する場合は、同様にしてチャネルRの基準位相に対してチャネルSの基準位相を検出したりする事も考えられる。

なお、本実施の形態17において、周波数拡散通信を例に説明を行ったが、これに限らず、O F D Mなどのマルチキャリア信号にも適用可能であるし、シングルキャリア信号でも可能である。O F D M通信においては、拡散、逆拡散がI F F T、F F Tに置き換え、チャネルをサブキャリアに置き換えることで容易に実現が可能である。O F D Mの場合、伝搬特性がサブキャリアの電力に現れるので、この包絡線をパラメータとして符号を割り当てるなどすればよい。

また、本実施の形態17において、伝搬を通じて合成された信号電力に情報を重畳する方式について説明を行ったが、これに限らず、当然信号の位相や周波数などにも重畳することは可能であり、さらに偏波や遅延プロファイルなどに情報を重畳することが可能であるといった特徴がある。

また、本実施の形態17において、アンテナの構成として偏波面の異なる（例えば偏波面が直交する）アンテナを配することで、前述の通り偏波に信号を重畳することも可能である。この場合には、特にマルチキャリア信号である必要はないが、マルチキャリア信号を用いる場合、チャネルRの偏波面を基準としてチャネルSの偏波面の角度に情報を重畳するなどが考えられる。

また、本実施の形態17において、遅延プロファイルに情報を重畳する場合、マルチキャリア信号を用いることで、チャネルRから得られる遅延プロファイルを基準として、チャネルSから得られる遅延プロファイルの差分に情報を重

疊することも考えられ、この様にすることで遅延プロファイルが対象とする伝搬状態の同一性が保たれるため、精度の高い通信が期待できるといった特長を有する。また、実施の形態 17において、同一時刻でかつ同一周波数に秘匿情報と疑似情報を重疊することによって、ターゲットとする受信位置でのみの通信を可能とし、秘匿性の高い通信方式を提供することができる。

(実施の形態 18)

本実施の形態 18は、上記実施の形態 17で説明した発明をさらに拡張して複数の受信信号系列から得られる夫々の伝搬パラメータに対して情報を重疊する点を特徴とするものである。

図 4 3 は、本実施の形態 18に係る通信装置である受信装置 4 3 0 0 の構成を示す図であり、図 4 4 は、本実施の形態 18に係る通信装置である送受信装置 4 4 0 0 の構成を示す図である。なお、図 9 及び図 3 6 と同一構成である部分には同一の符号を付してその説明は省略する。

本発明の実施の形態 18に係る通信装置である受信装置 4 3 0 0 は、図 3 6 に示す本発明の実施の形態 17に係る受信装置 3 6 0 0 において、受信部 3 6 0 2 の代わりに受信部 4 3 0 2 a、4 3 0 2 b を有し、逆拡散部 3 6 0 4 の代わりに逆拡散部 4 3 0 3 a、4 3 0 3 b を有し、復調部 3 6 0 5 の代わりに復調部 4 3 0 4 a、4 3 0 4 b を有している。

受信部 4 3 0 2 a 及び受信部 4 3 0 2 b は、受信装置 4 3 0 2 を構成している。逆拡散部 4 3 0 3 a 及び逆拡散部 4 3 0 3 b は、逆拡散装置 4 3 0 3 を構成している。復調部 4 3 0 4 a 及び復調部 4 3 0 4 b は、復調装置 4 3 0 4 を構成している。

受信部 4 3 0 2 a は、アンテナ 4 3 0 1 a から入力した受信 R F 信号を電力增幅及び周波数変換して逆拡散部 4 3 0 3 a へ出力する。

受信部 4 3 0 2 b は、アンテナ 4 3 0 1 b から入力した受信 R F 信号を電力增幅及び周波数変換して逆拡散部 4 3 0 3 b へ出力する。

逆拡散部 4 3 0 3 a は、受信部 4 3 0 2 a から入力した受信信号とチャネル

に対応する拡散符号とを畳み込み演算により逆拡散してチャネル信号を復調部 4304aへ出力する。

逆拡散部 4303b は、受信部 4302b から入力した受信信号とチャネルに対応する拡散符号とを畳み込み演算により逆拡散してチャネル信号を復調
5 部 4304b へ出力する。

復調部 4304a は、逆拡散部 4303a から入力したチャネル信号を復調してチャネル復調信号を選択合成部 4305 へ出力するとともに、通信制御部 4306 の出力指示信号にしたがって復調信号を電力検出部 3606 へ出力する。

10 復調部 4304b は、逆拡散部 4303b から入力したチャネル信号を復調してチャネル復調信号を選択合成部 4305 へ出力するとともに、通信制御部 4306 の出力指示信号にしたがって復調信号を電力検出部 3606 へ出力する。

選択合成部 4305 は、通信制御部 4306 から入力した選択合成信号に基づき、各アンテナから受信したブランチ受信信号（或いはブランチ受信データ）を選択（或いは合成）した後、選択合成結果を第 2 データとして出力する。この様にすることで、伝搬空間を時刻によって切り換える効果が得られるため、空間ダイバーシティのような利得が得られる。

通信制御部 4306 は、定められた時間に定められたアンテナからのブランチ受信信号（或いはブランチ受信データ）を選択・合成するように選択合成信号を選択合成部 4305 へ出力する。また、通信制御部 4306 は、秘匿情報が含まれている信号を受信したアンテナ 4301a、4301b の復調信号を電力検出部 3606 へ出力させるための出力指示信号を復調部 4304a、4304b へ出力する。これにより、第 3 者からは伝搬空間を推定することが不可能なため、アンテナ 4301a、4301b の通信信号を分離することが不可能であり、より高度なセキュリティを実現することが可能になると言った有利な特長がある。

比較部 3608（伝搬パラメータ差算出手段）は、アンテナ素子 4301a にて受信した受信信号の受信電力とアンテナ素子 4301b にて受信した受信信号の受信電力との差分（伝搬パラメータ差）を算出し、算出した差分情報を第 1 データとして出力する。

5 図 45 は、送信装置と受信装置に設けられたアンテナと、送受アンテナ間で決定される伝搬係数および、各アンテナから入出力される信号との関係を表した図である。図 45 は、図 38 の受信アンテナ数を 1 本から 2 本に拡張したものである。

10 以上のように構成されたシステムにおいて、アンテナ Ar1、Ar2 における受信信号は以下の式で与えられる。

$$\begin{aligned} S_{rx1}(t) &= \sum S_{tn} \cdot h_{1n} \\ &= \sum (\sum S_{cm} \cdot C_{mn}) \cdot h_{1n} \quad (29) \end{aligned}$$

$$\begin{aligned} S_{rx2}(t) &= \sum S_{tn} \cdot h_{2n} \\ &= \sum (\sum S_{cm} \cdot C_{mn}) \cdot h_{2n} \quad (30) \end{aligned}$$

15 式 (29)、式 (30) からも分かるとおり、 S_{rx1} と S_{rx2} は伝搬路の構成が異なるため、伝搬パラメータ h_{1n} 、 h_{2n} も異なってくる。これら S_{rx1} と S_{rx2} の受信状態は、式 (29)、式 (30) で示す C_{mn} の操作によって制御可能である。受信端末では、 S_{rx1} で得られる伝搬状態と S_{rx2} で得られる伝搬状態とを比較した結果を情報として復調・復号に供することも考えられる。則ち送信側では S_{rx1} と S_{rx2} で制御する伝搬パラメータの差分（位相差分や受信電力差などが考えられる）に対して情報を重畠させて送信し、一方受信側では S_{rx1} と S_{rx2} の各受信信号から求めた伝搬パラメータの差分を算出し、この差分を通信情報の一部或いは全部として通信することで通信する事により、より多様な通信を可能とする。さらにこの様にして通信を行うことで、2 系統分の伝搬パラメータを推定する必要性が生じ、そのため高度なセキュリティを確保することが可能になる。当然、アンテナの数を増加させることでより高度なシステムを構築可能であり、こうすることでセキュリ

ティの向上が見込める。

また、複数のアンテナ Ar 1、Ar 2 を用いてセキュリティ通信を行うことも可能である。アンテナ Ar 1 とアンテナ Ar 2 とは伝搬パラメータが異なるため、受信される信号が異なることは前述の通りである。このことを利用する
5 と、アンテナ Ar 1 に対する変調信号とアンテナ Ar 2 に対する変調信号を夫々制御することで、アンテナ Ar 1 に対してのみ秘匿情報を伝送したり、アンテナ Ar 2 に対してのみ秘匿情報を伝送したり、或いは両アンテナ Ar 1、Ar 2 に対して秘匿情報を伝送したり、これらの状態を定められた時間で切り換えたりする事で、より複雑で高度なセキュリティ通信を可能にする。

10 図 7 1 を用いて具体的に説明する。図 4 2 と同一の内容であるが、ターゲットとする場所が 1 箇所から 2 箇所に増えた場合を示している。図 4 2 には上下にグラフが分割されて記載されているが、図 4 2 と同様電波の電力分布を示したものである。上下のグラフは同一断面を表している。たとえば実施の形態 1
15 7 で説明したように、2 箇所にヌルを形成してこれを所定の時間で切り替えて出力した場合、上のグラフと下のグラフとが切り替わったようになるが、この
ようにして、受信機側でもそれに同期させて切り替えることによって実施の形
態 1 7 と同様に通信が可能になる。さらに、図 7 6 に示すようにヌルを対応す
る 2 箇所に形成して通信を実施すると、不要成分が両アンテナに入らないため
同様に通信が行えるようになる。さらに、アンテナ Ar 1、Ar 2 でそれぞれ
20 受信した信号は、伝搬係数を利用することで図中の太い実線と太い点線とを分
離可能になる。受信アンテナの数が n (Ar 1 … Ar n) であれば、時空間
多重 (S D M (Space Division Multiplex) や M I M O (Multi-Input
Multi-Output)) することで、図 4 2 に比べ通信容量を n 倍に拡大することも
可能である。当然、時空間符号化 (Space-Time Code) するこ
25 とで、特性の大幅な改善も見込まれる。このため、通信容量・通信品質の観点
から非常に有利な特長をもつ。

さらに、このように通信を行った場合、図 4 5 に示したようにチャネルを構

成するパラメータ要素が多くなるため、第3者へ情報が漏洩する危険性が大幅に減るといった大きな特長を有する。また、この秘匿通信をMIMOなどで利用されている空間分離用のパイロット信号や通信の位相・振幅の基準信号に対して実施しても同様の効果が得られる。

- 5 上記では、伝搬特性に応じてアンテナ係数（重み付け係数）を演算するとしたが、この計算方法について説明する。ここでは、n行×m列の行列Hを例に挙げる（則ち送信アンテナ数n、受信アンテナ数mの場合となる）。全ての行列Hは直交行列U（m行m列）、V（n行n列）と特異値行列S（n行m列）を用いて、

10 $U \times S \times V' = H \quad (31)$

ここで V' はVのエルミート転置を意味している。

この様に分解された直交行列U（或いはV）は $m \times 1$ ($1 \times n$) の特異値ベクトルをm (n) 個並べた行列であると見なし、これを $u_1 \sim m$ ($v_1 \sim n$) とする。

- 15 この時、 $u_1 \sim m$ ($v_1 \sim n$) は、

$$u_x \times H = \lambda x \quad (\text{または} H \times v_x = \lambda x) \quad (32)$$

である。 λx は u_x (v_x) に対応する特異値である。この時、伝搬特性を表す行列Hを特異値分解し、特異値 $\lambda x = 0$ である固有ベクトル u_x の各要素を

- 20 アンテナ係数（重み付け係数）とすることで受信アンテナ端での受信電力を0

に制御することが可能となる。

次に、図44を用いてより詳細に説明する。図44は、図9とほぼ同様の構成によって為されており、図44においてはベクトル量子化を行わないため、

図9の構成から符号化部105、コードブック905を除いたものとなっている。以下、図9との相違点のみについて説明する。伝搬推定部103は、受信

- 25 した受信信号から端末間の伝搬特性（伝搬行列H）を算出する。この伝搬特性は係数算出部903へ送出され、係数算出部903で伝搬行列Hの特異値分解を行う。このうち、対応する特異値 $\lambda x \neq 0$ である特異値ベクトル v_x ($x =$

1、 ……、 p)、 $\lambda x = 0$ である特異値ベクトル $v x$ ($p + 1$ 、 ……、 n) とする。ここでは便宜上前者を特異ベクトル、後者をゼロベクトルと呼ぶことにする。これらは全てバッファ 904 に一時保存される。一方、通信情報 1 ~ k が変調部 906 へと入力されそれぞれ対応する変調信号 1 ~ k が出力される。
 5 特異値ベクトルと変調信号はそれぞれ重み付け部 907 に入力され、秘匿化したい通信情報に対応する変調信号（ここで通信情報 1、変調信号 1 とする）と特異ベクトル ($v_1 \sim v_p$) のうちどれか（例えば特異値の最大のもの、或いは幾つかまたは全てを加算したベクトル）をベクトル乗算する。更に秘匿性を高めたい場合、受信装置に対して不要な通信情報（ここで通信情報 3、変調
 10 信号 3 とする）に対して、重み付け部 907 で乗ずる係数をバッファ 904 で保持された特異値ベクトルのうち、ゼロベクトル ($v_{p+1} \sim v_n$) のうちどれか（幾つか或いは全てを加算したベクトル）をベクトル乗算する。これらベクトル演算された変調信号ベクトルは送信部 908 に入力される。送信部 908 は、各変調信号ベクトルは対応するアンテナの信号系列毎に加算された後に
 15 周波数変換され、アンテナ 901 を介して放射される。

この様にして放射された信号は伝搬空間を介して受信装置で受信されるが、伝搬空間の特性（伝搬行列 H）と変調信号 $S \bmod$ を用いて以下のように表される。

$$H \times S \bmod \times v x = \lambda x \times S \bmod \quad (33)$$

20 数式 33 からわかるように、特異値ベクトルが乗算されている変調信号 1 は受信装置に届くことが分かる。一方、変調信号 3 は特異値 $\lambda x = 0$ であるベクトルが乗算されているため、受信装置には届かない。則ち、受信装置は受信信号をそのまま復調することで、変調信号 1 のみを復調することが可能になる。

以上のこととは、即ち図 42、71、76 に示したようなヌル制御を行っていることと等価である。つまり、ヌル制御によって秘匿通信を実施する場合は特異値分解を行い、これで得られる特異値ベクトルを活用することで容易に実施が可能であることを示している。

次に送受信装置でない第3の装置がこれらの信号を受信することを考えると、送信装置と共有する伝搬特性である伝搬行列 H' が異なるため、数式33は成り立たない。つまり、変調信号1、3は伝搬行列 H' と先の特異値ベクトルとの相関により与えられ、この信号を変調信号1と3とに分解することは不可能である。

また、秘匿化しない通信情報に対応する変調信号（ここで通信情報2、変調信号2とする）に関しては、重み付け部907で乗ずる係数をバッファ904で保持された特異値ベクトル以外（或いは[1, 1, ..., 1]のような一定のベクトル）の係数を与えればよい。この場合、特異値ベクトルと異なる係数を与えていたため、数式33は成り立たず、受信装置に受信される。

以上説明したように、送信装置において、送信する変調信号を送信相手である端末との間で形成されている伝搬状態（あるいは伝搬パラメータ）によって分解し、分解した信号をそれぞれのアンテナから送信することで、受信端での信号は空間合成により元の変調信号になる。このとき、変調信号の分解方法としては、伝搬パラメータから導出される係数（数式32の固有ベクトルの各要素に相当する値）をアンテナ係数（あるいは重み付け係数）として与え、元の変調信号とアンテナ係数との乗算によって行うことが可能である。この様にすることで、伝搬パラメータを共有できない第3の端末では空間合成の結果が異なるため、正しく復調できないという秘匿性を有する。

また、本通信方式の為に特別な構成を持たない受信装置であっても選択的な通信が行えることを示している。則ち、本発明は送信装置のみを変更することでセキュリティ通信を実現することが可能であると言った非常に大きな特長を有する。

このように、本実施の形態18の通信装置及び通信システムによれば、上記実施の形態1及び実施の形態17の効果に加えて、送信する変調信号を伝搬状態によって分解して各々の信号を異なるアンテナから送信するので、伝搬状態が異なる第3の端末では空間合成の結果が異なるために正しく復調できず、高

いセキュリティを確保することができる。また、本実施の形態18において、同一時刻でかつ同一周波数に秘匿情報と疑似情報を重畳することによって、ターゲットとする受信位置でのみの通信を可能とし、秘匿性の高い通信方式を提供することができる。

5

なお、本実施の形態18においては、アンテナAr1、Ar2が同一の端末に接続されていることを前提として説明したが、これに限らず、アンテナAr1、Ar2が夫々別の端末（例えば端末1と端末2）に接続されていても良い。こうすることで、端末1に対するセキュリティ通信と端末2に対するセキュリティ通信を同時に行うことも可能になり、効率の良いシステムを構築可能である。
10

（実施の形態19）

本実施の形態19は、受信信号に重畠されている伝搬特性を利用して端末特定を行う点を特徴とするものである。

15 図46は、本実施の形態19に係る受信装置4600の構成を示す図である。なお、図1と同一構成である部分には同一の符号を付してその説明は省略する。

特徴抽出部4601とバッファ部4602は、伝搬特徴抽出部4606を構成している。特徴抽出部4601は、伝搬推定部103から入力した伝搬推定情報より伝搬状態の特徴を抽出して特徴抽出情報をバッファ4602及び端末判定部4603へ出力する。バッファ部4602は、記憶した伝搬状態に応じた特徴抽出情報をバッファ情報として端末判定部4603へ出力する。
20

バッファ部4604及び情報処理部4605は、信号処理選択部4607を構成している。

特徴抽出部4601は、受信信号から得られた伝搬情報を入力して符号化することによりその特徴を抽出する。特徴を抽出する要素としては、位相特性、ゲイン特性、偏波特性、伝搬遅延特性、遅延分散特性、到来方向推定による角度プロファイルなどが挙げられる。これらの要素を単独あるいは要素の組み合

わせて得られる特徴をアナログ値として標本化しても構わない。この場合、特に特徴抽出する必要はなく端末判定部 4603 の判定もアナログ情報での比較となるためより高度で精度の高い判定が可能となる。一方、特徴を抽出する方法としてフーリエ変換やディスクリートコサイン変換、ウェーブレット変換などに代表される変換や、フィルタやマルチバンドフィルタなどのフィルタ、或いは線形予測法に基づく係数抽出などが考えられる。また、特徴抽出部 4601 は、図 1 などで用いられている符号化部 105 と同一の構成とすることも可能である。図 4 で示すように符号化部 105 をベクトル量子化の手法を用いることで、多様な信号系列を 1 つの符号として表すことが可能となるため、端末判定を行う際の比較が容易になると言った特長がある。

バッファ部 4606 は、抽出した特徴抽出情報を一時的に記憶して、所定のタイミングにて記憶した特徴抽出情報をバッファ情報として端末判定部 4603 へ出力する。

端末判定部 4603（判定手段）は、特徴抽出部 4601 から入力した特徴抽出情報とバッファ部 4606 から入力したバッファ情報を比較して一致具合を判定し、その判定結果を端末判定信号（第 1 データ）として情報処理部 4605 へ出力する。端末判定部 4603 は、一定時間で得られる伝搬情報を用いて最終的な端末判定結果を端末判定信号として 2 値信号で出力する。この場合、上述したように 1/0 のような 2 値信号ではなく 0~9 のような多値信号とすることでより柔軟なシステムを構成することも可能である。また、端末判定部 4603 は、特徴抽出部 4601 にて係数抽出する場合には、求められた係数列同士から両者のユークリッド距離を求め、その値が一定値以下であれば同一の端末であると判定し、そうでなければ異なる端末と判定する。判定の際、ノイズや伝搬特性の揺らぎなどにより判定結果が安定しない場合、一定の間判定結果を保存しておき一定時間の平均を取った後に判定する方法などが考えられる。そのような場合、判定結果を同一か異なるかを表す 0/1 の 2 値とするのではなく確からしさの値として 0~9 の様に幅を持たせることも考えら

れる。特に、端末判定を厳格に行おうとすると、結果に誤判定が出やすくなるため確からしさの値を一定期間で求められる平均値を元に判定を行うなどする事でより安定した端末判定が行える。このように、端末判定部 4603 は、
5 推定した伝搬環境に基づいて現在通信している端末を監視し、悪意により通信している端末が知らぬ間に入れ替わってしまうこと等により秘匿情報が漏洩してしまうことがないように監視している。

バッファ部 4604 は、復調部 104 より入力した受信データを一定期間記憶する。

情報処理部 4605 は、バッファ部 4604 に記憶されて入力した受信データ列と端末判定部 4603 から入力した端末判定結果とから情報処理の内容を切り換えて変更する。例えば、受信したデータのうち、端末に大きく依存するようなプライバシ情報や課金情報、秘匿情報などはその処理を行わずにエラー処理として受信データを全て破棄することが考えられる。他に、端末判定結果により違う端末からのアクセスであると判断された事を伝送し、セキュリティ対策処理を行うなどの方法が考えられる。
15

次に、受信装置 4600 の動作について説明する。

ここでは、端末特定を行う通信端末を通信端末 1、その通信相手を通信端末 2 として説明を行う。ここで、通信端末 2 が output した信号に対して、端末登録・
20 端末判定の動作を行うため、説明では端末 2 が output する場合のみについて説明する。

第 1 に、通信端末 1 は通信端末 2 の端末登録動作を行う。

通信端末 1 は通信端末 2 からの基準信号をアンテナ 101 で受信し、その RF 信号が受信部 102 に入力され受信信号が出力される。受信信号は伝搬推定部 103 に入力され受信信号と基準信号とから伝搬特性を推定し伝搬情報を出力する。
25 出力された伝搬情報は伝搬特徴抽出部 4606 へ入力され、特徴抽出部 4601 でその特徴抽出情報が出力される。この特徴抽出情報は、通信相手である通信端末 2 を特定する情報としてバッファ部 4606 に記憶される。

以上で、端末登録動作は完了する。

第2に、通信端末1は通信端末Xとの間で情報の授受を行うと共に、通信端末Xが登録された端末（通信端末2）であることの判定を行う。

通信端末1は通信端末Xからの通信信号をアンテナ101で受信し、そのRF信号が受信部102に入力され受信信号が出力される。受信信号は伝搬推定部103に入力され受信信号から伝搬特性を推定し伝搬情報を出力する。伝搬情報は特徴抽出部4601、受信部102及び復調部104へ出力される。受信部102では伝搬情報に基づいて周波数補正、時間補正、ゲイン補正などを行いながらRF信号から受信信号へ最適な状態を保つように制御される。復調部104は、受信信号を入力し、伝搬情報を元に周波数・位相補正、時間補正、ゲイン補正などを行いながら検波・復調し、受信データ系列を出力する。

次に、端末判定を行う場合の通信手順について、図47を用いて説明する。以下、端末特定を行う側を基地局（図47中では受信装置）、端末特定される側を端末（図47中では送信装置）として説明する。

15 (0) 基地局、端末：初期化

基地局、端末共に、電源が投入された直後、或いは特定の信号を受けて初期状態にセットされる。同時に、周波数や時間同期などの状態は事前に定められた手順に従ってセットされる。

20 以上のこれらの初期動作が終了した一定時間後、受信装置は一定時間毎に制御情報を制御信号に載せて送信する。

一方、基地局は初期動作が終了した後、制御信号のサーチを始める。端末が基地局から送信した制御信号を受信すると、その時刻、周波数などを検出してシステムが保有する時刻・周波数に同期する（システム同期）。システム同期が正常に終了した後、端末はその存在を基地局に通知するために登録要求信号を送信する。基地局は、端末からの登録要求に対して、登録許可信号を送信することで端末の登録許可を行う。

(1) 端末：基準信号送信

端末は、基地局で行う伝搬推定用の基準信号を基準信号として出力する。具体的な動作は、第1の実施の形態などで示した方法と同様の動作を行うが、基地局がこの通信で求めた伝搬情報からその特徴を抽出し、端末特定のための情報として求められた伝搬特性の特徴情報を該当する端末情報と共に登録する。

5 (2) 基地局：通信信号送信

基地局は、通信を開始し通信信号を出力する。暗号化通信を行う場合は他の実施の形態で述べた方法などを用いて暗号化信号を出力しても良い。

端末は、通信信号を受信すると受信復調部150が受信信号を復調情報へと復調し、復調データを出力する。通信に暗号化が行われていた場合、他の実施
10 の形態で述べた方法などを用いて復号する。

(3) 端末：通信信号送信

端末は、通信信号を送信する。基地局は、受信部102からの受信信号から伝搬特性を推定し、その伝搬情報から特長情報を抽出する。同時に受信信号の復調を行い、受信データを出力する。この特徴情報を(1)で登録した特徴情報とを比較し、端末の判定を行う。こうして得られた判定をまとめた最終判定結果の可・否情報を受信したデータを出力する。信号処理選択部4607では、受信データと端末判定信号を入力しそのうち受信データを一定期間バッファ部4604に記憶する。一方、端末判定部4603は一定時間で得られる伝搬情報を用いて最終的な端末判定結果を端末判定信号として2値信号で出力する。
20 情報処理部4605では、バッファ部4604に記憶された受信データ列と端末判定結果とから情報処理の内容を切り換える。例えば、受信したデータのうち、端末に大きく依存するようなプライバシ情報や課金情報、秘匿情報などはその処理を行わずにエラー処理として受信データを全て破棄することが考えられる。他に、端末判定結果により違う端末からのアクセスであると判断
25 された事を伝送し、セキュリティ対策処理を行うなどの方法が考えられる。

以下、(2)(3)の暗号通信や通常の通信を繰り返す。

以上の手順に基づいて通信を行うことで、受信信号とそれを出力した端末と

の照合が可能になる。特に端末判定を行う本方式については（2）の手順は必要ではなく、（1）および（3）の手順のみで実施することが可能である。

また、（3）の操作に於いて判定結果に基づいてその後の情報処理動作を変えて実施することも考えられる。このように判定結果に基づいて処理を切り換
5 えることにより、より処理の安全性を保つことが出来ると共に、正常に認証でき
ない端末によるデータ詐称などを防ぐことが可能となるため、非常に高いセ
キュリティを持った装置やシステムが構築できると言った特長を有すること
が出来る。

通信端末間に形成される伝搬路の特性は、端末の位置や周囲のレイアウトな
10 どで定まり、これを任意の特性に変更することは不可能である。複数のアンテ
ナを用いて伝搬を制御する方法も考えられるが、伝搬路特性は第3の端末から
は測定が不可能であり予測することも困難であるため、これを操作して通信端
末を詐称することは極めて困難であることが分かる。そのため、本発明を用い
た端末特定方法は、非常に簡単に高い精度で実現することが可能である。

15 さらに、アンテナ101と受信部102を複数用いて2つ以上の受信信号系
列から、2つ以上の伝搬路の特性を導き出すことで判定する端末との伝搬情報
が多様化するため、より高精度な判定を行うことが可能となる。

上記の方法によると、判定結果に誤判定が出た場合に通信の大幅なロスとな
ってしまう可能性がある。これを緩和して安定した通信を確保するためには、
20 端末判定で否の判断が為された場合、再確認を行うことも考えられる。この手
順について図47を用いて説明する。

（3'）端末：通信信号送信

基地局は、端末が出力した通信信号から得られる伝搬情報を利用して端末判
定を行う。（ここでは、（1）で登録した情報とは異なる結果が出たものと仮
25 定する）基地局は判定の結果、登録済みの端末とは異なる端末からの情報であ
ると判断し、受信データと共に否の端末判定信号を出力する。

（2'）基地局：要求信号

基地局は、端末判定の結果に従い端末の再確認を行うため、端末に対して認証要求信号を要求信号として出力する。

(1') 端末：基準信号送信

端末は、要求信号を受信するとそれに対応した動作を行う。ここでは基準信号を再度出力する。以下の手順は(1)～(3)と同様である。以上のような手続きを行うことで、伝搬環境の変化により誤った判定が起きる場合でも、再確認を行うことによって安定した通信を提供することが可能になる。

さらに、図46の信号処理選択部4607では判定結果が異なる場合、情報処理部4605の処理を一時停止し、(1')以降の再判定結果を待って情報処理の手順を決定することなどが考えられる。伝搬環境の変化に対応するためには、上記(3')～(1')の手続きとは別に、一定期間毎に基地局が登録した端末特定情報を更新することも考えられる。

また、(3)(3')の通信信号の一部に基準信号を挿入することにより、基地局が安定した伝搬推定を行うことが可能となるため、その結果として安定した端末判定結果が得られるといった効果がある。このとき、基準信号は(1)で用いる基準信号と同一である必要はなく、通信内で一般的に用いられるパイロット信号や既知信号系列などで代用可能である。

以上説明した本発明では、例えば通信が開始されてから終了するまでのセッションにおいて基地局・端末間で認証が完了してからセッションが終了するまでの間の情報について有効性を付する事が可能になる。例えばインターネットで課金情報などを授受する際にセッション途中で別端末が途中で詐称した信号を発信し、通信に悪影響を与えることを防ぐことが可能であるといった大きな特長を有する。

以上の説明では、伝搬を推定するために基準信号を用いるとしたが、通信している環境下において誤り検出可能な信号系列であれば良い。このような信号系列としては、パイロット信号、既知信号、シンクワード信号、同期信号、同期ワード、ブリアンブル信号、ミッドアンブル信号、ポストアンブル信号、リ

ファレンス信号、ユニークワード信号などが知られている。或いは、十分に復調エラーを保護された信号系列も用いることが可能であり、その例として例えば多値変調方式を通信している信号系列に含まれるPSK信号系列や、エラー訂正能力の高い方式で符号化された信号系列などが考えられる。

5 また、端末から基地局への通信の一部に端末を特定するIDを挿入し、その値と伝搬情報からの判定とを利用することも考えられる。

このように、本実施の形態19の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、端末判定部4603は、現在通信している端末が自分が希望する通信相手であるのか否かを伝搬推定値より判定し、自分が希望する通信相手ではない場合には端末判定結果に基づいて受信データを復調しない等の受信データの処理を切り換えるので、より処理の安全性を保つことが出来ると共に、正常に認証できない端末によるデータ詐称などを防ぐことが可能となるため、非常に高いセキュリティを持った装置やシステムが構築できる。

15 (実施の形態20)

図48及び図49は、伝搬パラメータに情報を多重するシステムにおいて具体的な通信フレームの設定方法を示した図である。なお、本実施の形態20における通信装置は、図7と同一構成であるのでその説明は省略する。

本実施の形態20は、便宜上下り回線を出力する装置を基地局、上り回線を出力する装置を端末として説明を行う。図48は上り回線と下り回線との信号出力タイミングを説明した図である。図48(a)は、セキュア情報を一方向で通信する場合であり、図48(b)は、セキュア情報を双方向で通信する場合である。なお、本実施の形態20においては、基地局と端末とは送受信装置700を備えているものとする。

25 最初に、一方向でセキュア情報を通信する場合について説明する。基地局は、端末に対して暗号化されていない通常の通信信号#4801を送信している場合において、端末から基地局へ上り回線を用いて基準信号#4802を含む

通信信号#4803が送信されてきた場合には、基準信号#4802に基づいて伝搬状態に応じた暗号鍵を選択し、選択した端末と共に暗号鍵を用いて暗号化した暗号化通信信号#4804を端末へ送信する。端末は、基準信号#4802を含む通信信号を所定の周期にて基地局へ送信する。基地局は、端末から送信された基準信号#4802を受信する度に暗号鍵が変更されていないか否かを確認し、確認後に暗号化信号#4805を端末へ送信する。

- 次に、双方向でセキュア情報を通信する場合について説明する。基地局は、端末に対して基準信号#4806を含む通信信号#4807を送信する。端末は、基地局に対して基準信号#4808を含む通信信号#4809を送信する。
- 10 基準信号#4808を受信した基地局は、基準信号#4808に基づいて伝搬状態に応じた暗号鍵を選択し、選択した暗号鍵を用いて暗号化した暗号化信号#4810を端末へ送信する。一方、基準信号#4806を受信した端末は、基準信号#4806に基づいて伝搬状態に応じた暗号鍵を選択し、選択した暗号鍵を用いて暗号化した暗号化信号#4811を基地局へ送信する。そして、
- 15 基地局は暗号化した暗号化信号#4812を端末へ送信する。

次に、図49を用いて基準信号を送信するタイミングについて説明する。図49はバースト構成の一例を示したものである。

- 図49(a)のフレーム構成は、バーストが通信信号と基準信号とで構成されている。基準信号は、例えばパイロット信号を用いる。この様に構成することで、伝搬特性を推定するための信号と、データを伝送するための基準信号を同時に送信することが可能となり、効率の良いフレーム構成が実現可能となる。また、基準信号の一部或いは全部を2シンボル以上連続した信号で構成することにより、伝搬特性を推定する場合に、伝搬特性の変化量の少ないシンボルを利用して推定が可能となるため、精度の高い伝搬推定を実現可能という特長を有する。また、基準信号を一定の間隔でバースト全体に配置することで、高速フェージングなどによりバースト内で伝送特性が大きく変動しても基準信号を基にフェージング歪を補正出来るため高品質の伝送を実現可能となる。この

のような高速フェージング環境下では、各実施の形態で述べたような端末間で形成される伝搬特性を利用した通信は、実現が困難となるため、高速フェージング状態を検知して互いの端末が伝搬特性を利用した通信を行うか行わないかの切り替えを行うことも可能となる。

- 5 図49(b)のフレーム構成は、図49(a)で示したフレーム構成の基準信号の一部或いは全部を基準信号1と基準信号2とすることとしたものである。この様に構成し、このバーストを送信する端末(端末1)が送信対象となる端末(端末2)に対して伝搬特性を利用して受信点において基準信号1の受信電力が基準信号2の受信電力より大きくなるように制御して通信を実施す
10 ることで、送信対象となる端末2では受信電力の違いから基準信号1を判断し通信信号の基準として正しく復調することが可能となるが、他の端末では場所によって夫々の受信電力が異なるため正しく復調することが不可能となるといった特長を有する。また、端末2のアンテナの数がn個ある場合、各アンテナに対して基準信号1～基準信号nを多重する事も考えられる。この様にすることで基準信号1～nの伝搬パラメータに対して情報を重畠することで高度な通信を可能にする。また、端末2がm個ある場合、夫々の端末に対する通信を空間多重することにより周波数利用効率を向上させることも可能になる。
(この場合、nとmとの間にはn>mの関係が成り立つ。)以上のようにすることで周波数利用効率の高いシステムを構築することが可能となる。
- 20 図49(c)のフレーム構成は、図49(a)で示したフレーム構成の通信信号の一部或いは全部を通信信号1と通信信号2とすることとしたものである。この様に構成し、端末1が端末2に対して伝搬特性を利用して受信点において通信信号1の受信電力が通信信号2の受信電力より大きくなるように制御して通信を実施することで、送信対象となる端末2では受信電力の違いから通信信号1を判断し復調することが可能となるが、他の端末では場所によって夫々の受信電力が異なるため正しく復調することが不可能となると言った特長を有する。通信信号は、データ、データシンボル、変調シンボル、データ変

調シンボル、フリーシンボルまたはユーザシンボルなどとも呼ばれることもあり、通信データによって変調されるシンボルの事を示している。

このように、本実施の形態20の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、基準信号の送信タイミングを変えるかまたは上5り回線と下り下線を選択して基準信号を送信することにより、効率良く暗号化した信号を送受信することができる。

なお、本実施の形態20においては、図48（b）、（c）において、受信電力の違いに着目して説明したが伝搬パラメータの一例として説明したにすぎず、通信信号1（基準信号1）と通信信号2（基準信号2）との伝搬パラメ10ータの差に情報を重畠することも考えられ、通信信号1と通信信号2を受信する端末2では通信信号1（基準信号1）を基準として伝搬パラメータの差を算出し、この結果を復調結果の一部或いは全部とすることも考えられる。また、本実施の形態20においては、図49（b）では基準信号を多重する場合について説明し、図49（c）では通信信号を多重する場合について説明したが、15当然基準信号と通信信号とを多重する事も可能であることは言うまでもない。

（実施の形態21）

図50は、伝搬パラメータに情報を多重するシステムにおいて具体的な通信フレームの設定方法を示した図である。なお、本実施の形態21における通信装置は、図36と同一構成であるのでその説明は省略する。

20 図50は、符号分割多重（CDM）のフレーム構成の一例を示したものである。

図50（a）のフレームは、パイロット信号とデータ信号とで構成されている。パイロット信号は、データ信号の位相や振幅の基準を示したものである。受信装置はデータ信号の復調時に、このパイロット信号から求められた位相や25振幅の情報を復調の基準とするほか、時間や周波数の同期・マルチバス状態などの伝搬状態を算出する。データ信号ではデータ1～n（nは1以上の整数）を符号分割多重してある。ここで、データ1～nには符号1～mが割り当てら

- れているものとする。端末 1 は推定した伝搬特性に応じてデータ 1 ~ n 夫々に
対して伝搬パラメータ（ここでは受信電力とする）を制御する。この時、受信
電力に情報を重畳させるようにして重み付けすると、端末 2 の受信端では、デ
ータ 1 ~ n の夫々の受信電力が制御された状態で受信される。これらの受信電
5 力は符号 1 ~ m で逆拡散した信号振幅として得られるため、その振幅情報から
重畳された情報を検出することが可能となる。ここでは、多重するデータ数を
n、符号の種類を m としたが、n と m との間には $n \geq m$ の関係が成り立つ。さ
らに端末 1 が制御する受信電力を 0 とすることで $n > m$ での通信が可能とな
る。さらに様に $m = 1$ の場合は、符号分割多重を行う必要はない。
- 10 図 50 (b) のフレームは、図 50 (a) のフレーム構成とは異なり、デ
ータ 1 ~ n にパイロット信号を符号分割多重したことを特徴としたものであり、
図 50 (a) のフレーム構成と同様に伝搬パラメータに情報を重畳させて伝送
することも可能である上、パイロット信号の位相や振幅を制御することも考
えられる。
- 15 図 50 (c) のフレームは、データ 1 ~ n にパイロット 1 ~ m を符号分割多
重したことを特徴としたものである。この構成を探ることにより、最大 m 個の
パイロット信号を夫々独立して制御可能となるため、例えばデータ 1 ~ j はパ
イロット 1 の位相や振幅を基準として変調され、データ $j + 1 ~ k$ はパイロッ
ト 2 の位相や振幅を基準として変調される等により、高度な通信システムが構
築可能となる。このようにすることで、複数の受信端末に対して、それぞれの
20 パイロット信号とそれに対応したデータ信号とで独立に通信を行うことが可
能であり、かつ夫々のパイロット信号は通信相手とする受信端末の受信端にお
いて正しい信号基準となるように制御されていることから、受信端末同士が他
のデータ信号を受信し復調しようと試みても正常に復調できないと言った大
きな特長が得られる。通信信号は、データ、データシンボル、変調シンボル、
25 データ変調シンボル、フリーシンボルまたはユーザシンボルなどとも呼ばれる
こともあり、通信データによって変調されるシンボルの事を示している。

このように、本実施の形態2 1の通信装置及び通信システムによれば、上記実施の形態1の効果に加えて、パイロット信号とデータを符号分割多重するので、干渉に強い暗号化信号の送受信を行うことができる。

なお、本実施の形態2 1においては、パイロット信号を用いてデータ信号の位相や振幅の基準にすることとしたが、これに限らず、パイロット信号以外の基準信号を任意に選択することができる。

(実施の形態2 2)

図5 1は、本発明の実施の形態2 2に係る通信装置である送受信装置5 1 0 0の構成を示す図である。送受信装置5 1 0 0は、図2に示す本実施の形態1 10に係る送受信装置2 0 0において、直交周波数分割多重部5 1 0 1を追加するものである。なお、図2と同一構成である部分には同一の符号を付してその説明は省略する。

切換部2 1 0は、送信信号が後述する直交周波数分割多重部5 1 0 1にて直交周波数分割多重処理された後の送信信号が各サブキャリアに対して所望の配置となるように暗号化部2 0 9から出力される暗号化されたセキュリティデータと基準信号生成部2 0 8から出力される基準信号とを切り替えて変調部2 1 1へ出力する。

直交周波数分割多重部5 1 0 1は、変調部2 1 1から入力した送信信号を直交周波数分割多重処理して送信部2 1 2へ出力する。即ち、直交周波数分割多重部5 1 0 1は、変調部2 1 1から入力した送信信号を、パラレルデータ形式からシリアルデータ形式に変換して逆高速フーリエ変換した後にパラレルデータ形式からシリアルデータ形式に変換して送信部2 1 2へ出力する。直交周波数分割多重処理された送信信号は、各サブキャリアに振り分けて配置される。

図5 2は、直交周波数分割多重(O F D M)のフレーム構成の一例を示したものである。縦軸は周波数、横軸は時間を表しており、1つの枠は1シンボル中の1サブキャリアを表している。

図5 2(a)のフレームは、シンボル同期用のパイロット信号、データ復調

用の基準信号及びデータ送信用のデータ信号から構成されている。シンボル同期用のパイロット信号は、O F D Mシンボルの時間と周波数の同期を行うために用いられ、ヌルシンボルやショートワードシンボル、ロングワードシンボルなどが知られる。一方、データ副長用の基準信号は、伝搬歪により発生する周波数特性や伝搬遅延・位相回転などを補正するために挿入されるものであり、変調されるデータ信号の位相や振幅の基準を与える。フレーム内にこの基準信号を挿入することにより伝搬環境が変化したり、遅延プロファイルが変化したりする環境においても安定した通信を可能にする。本発明により、基準信号を伝搬特性に対応して、受信端における位相や振幅を制御して传送する事により、
5 設定した受信端以外の場所では正しい基準信号が得られないため、正しい復調を行うことが困難になると言った大きな特長を有する。

図52 (b) のフレームは、図52 (a) のフレーム構成と同様にシンボル同期用のパイロット信号、データ復調用の基準信号及びデータ信号とからなっている。特定のシンボルで基準信号を送信する図52 (a) のフレーム構成に
15 対して全シンボルの一部が基準信号となっていることから、シンボルに対応して基準信号を変化させることが可能となる。則ち、シンボルの切替時に伝搬特性を利用した制御係数を変化させて基準信号が示す位相や振幅の値を時々刻々と変化させることで、より複雑な制御が可能となりセキュリティシステムにおいては、高度なセキュリティが確保できるといった特徴を有する。また、
20 基準信号は既知信号であることからパイロット信号としても利用することが可能であり、こうする事で環境の時間変化に対して補正がかけられるといった特徴を有する。

図52 (c) のフレームは、図52 (b) のフレーム構成の基準信号を時刻によって変化させることが特徴である。基準信号の位置が刻々と変化することで、基準信号やデータ信号に対して周波数ホッピングの効果が現れる。則ち、伝搬状態によるノッチによって一定のサブキャリアの電力が低くなつたとしても信号パターンが切り替わるため、ノッチによる影響は一時的なものに抑え

られる。例えば、基準信号の箇所がノッチによって影響を受けてしまうとデータ信号に対して大きな影響がある上、フレーム構成 2 であれば伝搬状態が変化するまではその影響が続いてしまうが、本構成であれば基準信号の影響を限定的にすることが可能となる。通信信号は、データ、データシンボル、変調シンボル、データ変調シンボル、フリーシンボルまたはユーザシンボルなどとも呼ばれることもあり、通信データによって変調されるシンボルの事を示している。

このように、本実施の形態 2 2 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、直交周波数分割多重部 5 1 0 1 は、暗号化されたデータ及びパイロット信号を直交周波数分割多重処理して各サブキャリアに配置するので、暗号化信号を送信する際の周波数利用効率を高くすることができる。

(実施の形態 2 3)

本実施の形態 2 3 は、上位層の指示によりセキュリティ通信を行うか否かを決定する点を特徴とするものである。

図 5 3 は、本実施の形態 2 3 に係る送受信装置の構成を示す図である。なお、図 7 と同一構成である部分には同一の符号を付してその説明は省略する。

通信制御部 5 3 0 1 は、通信時刻に応じて通信方法の切り換え・合成の制御を行う。即ち、通信制御部 5 3 0 1 は、上位層 5 3 0 3 からセキュア通信を行うための通信制御信号が入力した場合には、符号化部 7 0 3 から入力した伝搬情報を伝搬制御部 7 0 1 へ出力し、さらに受信部 2 0 2 へセキュア通信を行う旨の受信制御信号を出力するとともに送信部 7 0 5 へセキュア通信を行う旨の送信制御信号を出力する。一方、通信制御部 5 3 0 1 は、セキュア通信を行わない旨の通信制御信号が入力した場合には、受信部 2 0 2 へセキュア通信を行わない旨の受信制御信号を出力するとともに送信部 7 0 5 へセキュア通信を行わない旨の送信制御信号を出力する。伝搬制御の方法については、セキュリティ通信を行う場合は他の実施の形態で示したような伝搬制御を行い、従来の通信方法を行う場合は伝搬制御をせずに通信したり、或いは伝搬制御として

指向性を絞って通信品質の向上を図る事も考えられる。

バッファ部 5302 は、送信データを一時的に保持して切換部 210 へ出力する。

上位層 5303 は、通信のレイヤ構造で言う L1 より上位にあたる部位（データリンク層、ネットワーク層、トランスポート層、セッション層、プレゼンテーション層、アプリケーション層のうちのどれか）となる。上位層部では、受信データや送信データの入出力を行うと同時に、必要に応じて通信方法の選択が行われその制御信号を、それを通信制御信号として出力する。

本発明を用いた通信方法は、従来の通信方法と親和性が高く両者の通信方法を切り換えて利用することも可能である。この様にすることで、

- (1) 通信相手である通信装置がセキュリティ通信をサポートしているかどうか
- (2) アプリケーションが本発明の通信方法をサポートしているかどうか
- (3) アプリケーションが本発明の通信方法を必要としているかどうか
- (4) ユーザが本発明の通信方法を必要としているかどうか

などの状況に応じて従来の通信方法か、本発明を用いた通信方法かを切り換えることも可能である。更に、他の実施の形態でも述べたようにセキュリティ通信を必要とする場合でも、重要な情報だけをセキュリティ保護して通信を施すことによって通信品質を確保出来ると言った事も考えられる。

次に、図 53 に示す送受信装置の動作について、図 54 を用いて説明する。

上位層部からセキュリティ通信を実施するように通信制御信号が出されると、通信制御部がセキュリティ通信用に伝搬制御を行なうように送信・受信制御信号を出力する。（図中の（1）、（4））一方上位層部からセキュリティ通信を実施しないように通信制御信号が出されると、通信制御部がセキュリティ通信用に伝搬制御を行わないように送信・受信制御信号を出力する。（図中の（2）、（3）、（5））

このように、本実施の形態 23 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、通信制御部 5301 は、上位層 5303 の指示

により、伝搬推定値を用いて第1データの送受信を行う通信方式である重要な情報をセキュリティ保護したセキュリティ通信方法と従来の通信方式とを切り替えて送信するので、汎用性のある通信装置を提供することができる。

なお、本実施の形態23においては、送信制御信号及び受信制御信号によつて受信部202や送信部705の伝搬制御をON/OFFするとしたが、これに限らず、受信部202または送信部705のどちらかが従来の通信装置の該当部位と同一の構成である場合、その部位に対する制御信号は不要である。例えば、図1に示した通信装置の送信部152や、図7に示した通信装置に対応する通信装置の暗号受信部706などがこれに相当する。

10 (実施の形態24)

本実施の形態24は、アンテナ係数に秘匿情報を含めるようにする点を特徴とするものである。

図55は、本実施の形態24に係る通信装置である送信装置5500の構成を示す図であり、図56は、本実施の形態24に係る通信装置である受信装置5600の構成を示す図である。

最初に送信装置5500について説明する。

変調部5501は、第2データを一時的に保持してチャネル数分のチャネル位相変調信号を合成部5502へ出力する。

合成部5502は、伝搬変調部5507より入力した変調アンテナ係数に従って変調部5501から入力した変調信号との合成演算が行われる。

送信部5503は、合成部5502から入力した合成信号を周波数変換及び電力増幅等する。

アンテナ5504は、対応する系列の信号を放射する。

伝搬特性格納部5505は、遅延プロファイル等の伝搬特性を格納してアンテナ係数算出部5506へ出力する。

アンテナ係数算出部5506は、アンテナ係数に代表される伝搬状態に情報を重畠するために、伝搬特性格納部5505から入力した伝搬特性に基づいて

アンテナ係数を算出する。アンテナ係数の求め方は様々であるが、特異値分解などが知られている。

伝搬変調部 5507 は、アンテナ係数算出部 5506 から入力したアンテナ係数と秘匿情報として送信する第 1 データを重畳して振幅変調した変調アン

5 テナ係数を合成部 5502 へ出力する。

次に、受信装置 5600 について説明する。

アンテナ 5601 は、受信 R F 信号を受信部 5602 へ出力する。

受信部 5602 は、アンテナ 5601 にて受信して入力した受信 R F 信号を電力増幅及び周波数変換等して復調部 5603 へ出力する。

10 復調部 5603 は、受信部 5602 から入力した各チャネル信号を復調してチャネル復調信号をアンテナ係数検出部 5605 とバッファ 5604 へ出力する。受信装置 5600 では位相変調に振幅変調が加えられた Q A M 信号（或いは位相・振幅変調信号）が受信されることになるため、復調部 5603 は、受信信号を位相・振幅復調する。

15 バッファ 5604 は、復調部 5603 から入力したチャネル復調信号を一時的に保持して第 2 データを出力する。

アンテナ係数検出部 5605 は、復調部 5603 から入力したチャネル復調信号よりチャネル毎にアンテナ係数を検出し、検出したアンテナ係数情報を比較部 5606 へ出力する。

20 比較部 5606 は、アンテナ係数検出部 5605 から入力したアンテナ係数情報を符号化し、符号化したアンテナ係数情報の大きさを比較した結果を第 1 受信データとして出力する。なお、送信装置 5500 及び受信装置 5600 の動作は、受信電力の代わりにアンテナ係数を用いる以外は図 37 と同一であるのでその説明は省略する。

25 本発明の伝搬特性に情報を重畳する場合、アンテナから出力される変調方式と受信装置が復調する変調方式が異なる点が大きな特徴である。換言すれば、アンテナから出力する信号の変調方式が、受信装置のサポートする変調方式と

異なるように設定することも可能である。このようにすることで、送信対象となる受信装置に対してのみ正しい変調信号となり、他の受信装置では正しい変調信号が得られないため、高度な秘匿性を確保できる。また、複数チャネルの信号におけるアンテナ係数差の情報に秘匿情報を含めることができるので、高いセキュリティが確保できるとともに、複数チャネルの信号を伝送することができるので、伝送効率を向上させることができる。

10 このように、本実施の形態 24 の通信装置及び通信システムによれば、上記実施の形態 1 の効果に加えて、合成部 5502 は、伝搬変調部 5507 にて変調した第 1 データと変調部 5501 にて伝搬変調部 5507 とは異なる変調方式により変調した第 2 データとを合成し、送信部 5503 は、位相、振幅または周波数を組み合わせた変調方式にて第 1 データと第 2 データを送信するので、変調方式が異なる通信相手は復調することができないため、高いセキュリティを確保することができる。

15 なお、本実施の形態 24 においては、アンテナ出力信号を位相変調とともに伝搬変調を振幅変調としたが、これに限らず、両者が同じ変調方式でも良く、また変調方式もこれに限ったものではない。それぞれは、周波数変調、位相変調、振幅変調、PWM、PAM、直交振幅変調、CCK (Complementary Code Keying) などが考えられる。

(実施の形態 25)

20 本実施の形態 25 は、拡散処理した複数チャネルの信号にアンテナ係数情報を重畳してアンテナ係数情報を秘匿データとして取り出す点を特徴とするものである。

25 図 57 は、本実施の形態 25 に係る通信装置である送信装置 5700 の構成を示す図であり、図 58 は、本実施の形態 25 に係る通信装置である受信装置 5800 の構成を示す図である。なお、図 57 及び図 58 において、図 55 及び図 56 と同一構成である部分には同一の符号をしてその説明は省略する。

拡散符号格納部 5701 は、チャネル数分の拡散符号を格納して拡散部 57

02へ出力する。

拡散部5702は、変調部5501から入力した第1データであるチャネルデータと拡散符号格納部5701から入力したチャネルに対応する拡散符号を畳み込み演算し周波数拡散を行って合成部5502へ出力する。

- 5 拡散符号格納部5801は、チャネル数分の拡散符号を格納して逆拡散部5802へ出力する。

逆拡散部5802は、拡散符号格納部5801から入力したチャネルに対応する拡散符号と受信部5602から入力した受信信号とを畳み込み演算により逆拡散しチャネル信号を復調部5603へ出力する。なお、送信装置57010及び受信装置5800の動作は、受信電力の代わりにアンテナ係数を用いる以外は図37と同一であるのでその説明は省略する。

本発明の伝搬特性に情報を重畠する場合、アンテナから出力される変調方式と受信装置が復調する変調方式が異なる点が大きな特徴である。換言すれば、アンテナから出力する信号の変調方式が、受信装置のサポートする変調方式と異なるように設定することも可能である。このようにすることで、送信対象となる受信装置に対してのみ正しい変調信号となり、他の受信装置では正しい変調信号が得られないため、高度な秘匿性を確保できる。

このように、本実施の形態25の通信装置及び通信システムによれば、上記実施の形態1及び実施の形態24の効果に加えて、合成部5502は、伝搬変調部5507にて変調した第1データと変調部5501にて伝搬変調部5507とは異なる変調方式により変調して拡散処理した第2データとを合成し、送信部5503は、位相、振幅または周波数を組み合わせた変調方式にて第1データと第2データを送信するので、周波数利用効率の高いデータについて高いセキュリティを確保することができる。

25 なお、本実施の形態25においては、アンテナ出力信号を位相変調とともに伝搬変調を振幅変調としたが、これに限らず、両者が同じ変調方式でも良く、また変調方式もこれに限ったものではない。それぞれは、周波数変調、

位相変調、振幅変調、PWM、PAM、直交振幅変調、CCK (Complementary Code Keying) などが考えられる。

(実施の形態 26)

本実施の形態 26 は、アンテナ係数を制御することで一次変調に二次変調を

- 5 重畠する点を特徴とするものである。

図 68 は、本実施の形態 26 に係る通信システムを示す図であり、図 69 は送受に係る部位を詳細に示したものである。まず、図 68 について説明する。

図 68 で示すシステムでは、伝搬空間 6852 を介して通信端末 A 6850 と同一に構成された通信端末 B 6851 とでなっている。なお、図 68 では同一端末であるものとして示したが、この構成については同一端末である必要はない。

通信端末 A 6850 および通信端末 B 6851 について説明する。

参照信号格納部 6801 は、時間同期、周波数同期や位相・振幅などの基準を与える参照信号を出力する。

15 変調部 6802 は、データ 2 (第 2 データ) を入力して所定の変調信号を生成し変調信号を出力する。

チャネル合成部 6803 は、変調信号とチャネル成分を抽出したチャネルパラメータ、データ 1 (第 1 データ) とを入力し、伝搬を通じてチャネル合成を行うように信号の重み付けを行い、送信 RF 信号を出力する。

20 チャネル解析部 6804 は、受信信号から抽出した伝搬係数を入力してこれを解析しチャネル合成するための係数を算出、出力する。

受信復調部 6805 は、受信 RF 信号を入力して、その伝搬係数をチャネル解析部 6804 に出力するとともに、復調してデータ 1、2 を出力する。

RF 部 6806 は、送信 RF 信号をアンテナ 6807 へ出力するとともに、
25 アンテナ 6807 で受信した信号を入力して受信復調部 6805 へ受信 RF 信号を出力する。

アンテナ 6807 は、対応する系列の送信 RF 信号を放射、あるいは受信し

た受信R F信号を受信復調部6 8 0 5へ出力する。

スイッチ6 8 0 8は、チャネル合成部6 8 0 3に出力する変調信号を参照信号格納部6 8 0 1からの信号とするか、変調部6 8 0 2からの信号とするかを選択し、出力する。

- 5 制御部6 8 0 9は制御信号を入力し、チャネル合成部6 8 0 3、チャネル解析部6 8 0 4、受信復調部6 8 0 5、スイッチ6 8 0 8の制御を行う。具体的には、実施の形態2 3に記載したように上位層からの制御信号を受け、秘匿通信を行うか否かの設定を行ったり、実施の形態1などに記載の通信手順に応じて伝搬推定信号の出力や、規定されている通信フレームに準じた動作の制御を
10 行う。

送受信部分の詳細を記載した図6 9について説明する。図6 9は、図6 8の一部を詳細に示したものであり、同様の構成部位については同一符号を付してある。ここでは、各部位の説明は省略し、動作の詳細について説明する。

- データ（データ1～n）を入力した変調部6 8 0 2はそれぞれ対応するデータから変調信号1～nを生成し、チャネル合成部6 8 0 3へ出力する。チャネル合成部6 8 0 3には、変調部6 8 0 2から変調信号を入力するとともに、チャネル解析部6 8 0 4からチャネルパラメータをアンテナ係数として入力する。チャネル解析部6 8 0 4は、制御信号とR F部6 8 0 6で受信した受信信号を入力し、受信信号系列と参照信号などの既知信号系列などをを利用して位相や振幅、遅延分散など伝搬特性の特徴を抽出しそのチャネルパラメータをチャネル合成部6 8 0 3へと出力する。

- チャネル合成部6 8 0 3はチャネルパラメータと変調信号とからアンテナ系列に対応したアンテナ係数を算出する。また、制御信号により伝搬制御が必要であれば、このようにして算出したアンテナ係数と、変調信号とを掛け合わせ重み付けした送信信号を対応するR F部6 8 0 6へ出力し、ここで電力増幅されてアンテナ部6 8 0 7から放射される。

一方、伝搬制御が必要でない場合は、通信に適した（即ち受信点で最大感度

となるような信号になるよう) 制御を行ったり、重み付け係数を予め設定されてある値にセットしたり、あるいは 1 つ以上の係数を 0 にセットしたりする。

通信に適した制御を行った場合、通信品質が向上されるという特長がある。重み付け係数を予め設定してある値にセットする場合、たとえば通信環境がほぼ

- 5 固定であり、指向性が予め設定できるような状況であれば複雑な制御を行わず
に高い通信品質が向上するといった特長がある。このように事前に指向性を予
め設定できない場合は、全てを同一値に設定することでトータルの出力電力を
向上させることとなり通信品質の向上につながる。重み付け係数の一部を 0 に
セットする場合、出力電力の抑制になり、消費電力の低減が可能になる。

- 10 重み付け操作に関しては図 3 5 に示したような構成で可能である。ここで、
重み付けされる変調信号とアンテナ係数の算出時に用いる変調信号とを明確
に分離することで、情報の階層化が容易に実現できることは明らかである。

(このとき前者を一次変調、後者を二次変調と呼ぶことにする) このようにす
るとき、変調信号 1 ~ k を一次変調、変調信号 k + 1 ~ n を二次変調とするこ

- 15 とで可能である。たとえば実施の形態 1 7 で示したように、1 つの変調信号以
外はすべて電力が 0 となるように制御するという方式の場合、二次変調として
(1, 0) の変調信号に一次変調した変調信号 1 ~ k を、同様に二次変調とし
て (0, 0) の変調信号に一次変調した変調信号 k + 1 ~ n を適用していると
みなすことも可能である。このように二次変調である変調信号のパターンが少
20 ない場合、アンテナ係数をパターン数だけ用意しておきこれを二次変調に対応
するデータで切り替えることで実現が可能である。

ここで、アンテナ係数は数式 3 4 で与えられる。

$$H \cdot W(x) = x \quad (34)$$

- 25 数式 3 4 での x は二次変調で情報を重畠する成分であり、A S K であれば振
幅、P S K であれば位相、F S K であれば周波数となる。

こうして放射された電波は、伝搬空間 6 8 5 2 を介して通信端末 B 6 8 5 1
のアンテナ 6 8 0 7 で受信される。この信号はチャネル合成部 6 8 0 3 によっ

てチャネルパラメータが重畠されており、受信信号 S_{rx} は一次変調信号 S_t_1 、二次変調信号 S_t_2 、チャネル特性 H 、およびアンテナ係数 W を用いて数式 35 のように表すことが可能である。

$$S_{rx} = H \cdot W (S_t_2) \cdot S_t_1 \quad (35)$$

5 数式 34 を用いることで次式が得られる。

$$S_{rx} = S_t_2 \cdot S_t_1 \quad (36)$$

数式 36 で示された通り、通信端末 B6851 の受信端において、一次変調信号と二次変調信号とが掛け合わされた信号として受信信号が得られる。例えば一次変調を PSK 変調、二次変調を ASK 変調とすることで、受信復調部 6810 05 では、位相成分を検波することで一次変調に対応するデータ 2 を、振幅成分を検波することで二次変調に対応するデータ 2 を復調することが可能となる。

以上の説明を、図 70 を用いて更に詳細に説明する。

図 70 は、図 69 をより具体的に示したものであり、図中の 7050 ~ 7052 に信号のコンスタレーションを記述してある。

重み付け乗算部 7001 は、一次変調信号とアンテナ係数とを乗算した重み付け送信信号を出力する。

係数格納部 7002 は、チャネル解析部 6804 が算出したチャネルパラメータを入力し、これを基本係数として保持する。保持した基本係数は二次変調信号に応じて係数をアンテナ係数に変換され出力される。このとき、上述の通り二次変調のパターンが少ない場合は、基本係数をそのパターン数用意しており、二次変調に対応するデータ 1 に応じてアンテナ係数を切り替えることで容易に実現が可能となる。

ここで、一次変調を QPSK、二次変調を ASK として説明する。信号 7050a は、QPSK のコンスタレーション、信号 7050b は ASK のコンスタレーションを示している。

チャネル合成部 6803 では、係数格納部 7002 から出力されたアンテナ

係数を用いて一次変調信号の重み付けを行い、対応するアンテナ 6807へ重み付け送信信号を出力する。このアンテナ係数は、二次変調のシンボル ‘space’ と ‘mark’ では、位相・振幅とも異なるため、一次変調信号が 4 つの信号点を有していたのに対して、それぞれの重み付け送信信号では 8 つの
5 信号点を有していることになる。

ここで、二次変調信号の ‘space’ 、 ‘mark’ に対するアンテナ係数は、位相・振幅が異なることとしたが、どちらかを一定値として固定することも可能である。振幅を一定にした場合、各アンテナから供給する電力が等しくなるといった特長を有する。位相を一定にした場合、重み付け乗算部 700
10 1 の構成が容易になるといった特長を有する。

信号 7052 は、伝搬空間 6852 を介して通信端末 B6851 で受信された信号を示しており、式 36 で示されたように、QPSK に ASK を重畠した 8-APSK 信号のようになる。受信復調部 6805 は、位相を検波することで、データ 2 を、振幅を検波することでデータ 1 を復調することが可能である。
15

この様に本実施の形態 26 によると、アンテナ係数を制御することで一次変調に二次変調を重畠し、この変調信号は受信点でのみ正しい変調信号を形成することから秘匿性の高い通信を可能にすることを特長とするものである。

(実施の形態 27)

20 本実施の形態 27 は、上位層の通信において物理層での秘匿通信の制御を行う通信プロトコルについて記載したものである。

図 59 は、実施の形態 27 に用いる通信システムを示したものである。

通信システムは、通信端末 A5950 と通信端末 B5951 が伝搬空間 5952 を介して通信を行っている。ここで、通信端末 A5950 と通信端末 B5951 は同一の構成でなっている。
25

通信端末 A5950 について説明する。

上位層 4750 はアプリケーション（端末外部からの場合や端末内部の場合

が考えられる)と受信情報と送信情報を授受し、送信データを送信部152、制御信号を通信制御部4701へ出力し、受信データを受信復調部150から入力する。

受信復調部150は、アンテナ101から受信RF信号を入力し、それを復
5 調して受信データを出力する。

送信部152は、送信データを入力し変調信号を生成して送信RF信号をア
ンテナ101へ出力する。

通信制御部4701は、制御信号を入力し送信部152へ送信制御信号を、
受信復調部150へ受信制御信号を出力する。また、受信復調部150から伝
10 搬パラメータを入力し、送信部152へ伝搬パラメータを出力する。

アンテナ101は、送信部152から送信RF信号を入力しこれを放射し、
受信した受信RF信号を受信復調部150へ出力する。

通信において必須となるチャネル制御や時間制御などの通信制御は通信制
御部4701が行うが、それに加えて上位層からのコマンドは、制御信号を介
15 して通知される。コマンドを受けた通信制御部4701は、送信制御信号や受
信制御信号を通じて物理層のコマンド発行や秘匿通信制御などを行う。

以上の構成に基づいて、通信手順について図61を用いて詳細に説明する。
ここでは、実施の形態1で説明した秘匿通信に基づいて説明するが、これに限
らず他の実施の形態で説明した秘匿通信についても適用可能であることは言
20 うまでもない。

(0) 初期化

通信端末A5950および通信端末B5951は、電源投入時や通信開始時
などで、所定の手順に基づき初期状態に設定するため、上位層から初期化の制
御信号を出力する。

25 (0.a)、(0.b) 上位層から受けた制御信号に基づき、通信端末A5
950は物理層に関する設定状態を初期化する。

(1) セキュア情報送信

(1. 0) 通信端末Aのアプリケーションが上位層にセキュア情報とそれを送信する要求を出力する。

(1. 1) 通信端末Aの上位層はセキュア送信要求を受けると、物理層に対してセキュア情報とともにセキュア送信コマンドを発行する。

5 (1. 2) 通信端末Aの物理層はセキュア送信要求コマンドを受けると、端末A・B間での通信タイミングに合わせてセキュア通信コマンドを端末Bへ送信する。

(1. 3) 通信端末Bの物理層では、セキュア通信コマンドを受信すると、通信タイミングに従ってセキュア通信要求を伝搬推定用信号とともに通信端
10 末Aへ送信する。

(1. 4) 通信端末Aの物理層では、セキュア通信要求を受信すると伝搬推定用信号から伝搬を推定し、伝搬パラメータを算出する。さらに伝搬パラメータを用いて(1. 2)で入力したセキュア情報を、秘匿通信方法を用いて通信端末Bへ送信する。

15 (1. 5) 通信端末Bの物理層では、秘匿通信方法を用いて伝送されたセキュア情報を受信・復調し、その情報を上位層へ出力する。

(1. 6) 通信端末Bの上位層は物理層から出力されたセキュア情報を、アプリケーションへ出力する。

以上の一連の動作により、通信端末Aのアプリケーションから通信端末Bの
20 アプリケーションへセキュア情報が本発明の秘匿通信を用いて伝送される。本手順に従うことで、アプリケーション同士での通信手順を最も簡単に送信することが可能である。

以上の動作において、物理層における実際の通信信号について図64を用いて説明する。図中で網掛けされた部分は、通信端末Bから通信端末Aへの信号、
25 他は通信端末Aから通信端末Bへの信号を示している。セキュア通信コマンドが発行されると(1. 2)、所定の間隔(T_{guard})後にセキュア通信要求が伝搬用推定信号とともに受信される(1. 3)。この伝搬用推定信号を用

いて算出した伝搬パラメータに基づき、セキュア通信が実行される(1.4)。

ここで、図中に示した時間について説明する。

T_{guard} は通信信号の衝突を避けるために設けられた時間であり、一般にサポートする通信距離から求められる。

5 T_{access} はセキュア通信コマンドを発行してからセキュア通信が完了するまでの時間を表しており、上位層ではセキュア通信を行う際にこの値を用いて通信状態の管理を行うことが可能である。

T_{ready} はセキュア通信要求(伝搬推定用信号)が与えられてからセキュア通信が終了するまでの時間である。他の実施の形態でも示している通り、

10 本発明は伝搬パラメータを通信に用いているため、伝搬環境に変化がないことを前提としており、伝搬環境に変化が起きた場合通信品質の劣化を招く。この影響について図72～74を用いて説明する。

図72は、伝搬パラメータの直交性の時間的変化を表しており、所定の時刻における伝搬環境からの変化を直交性という指数で表現したものである。縦軸15は指数の大きさを、横軸はシンボル時間を示している。すなわち特定の時刻($t = 0$)の伝搬状況から特異値分解で求めた直交ベクトルと実際の伝搬状況との直交度合いを示しており、0であれば、伝搬パラメータと伝搬状況が一致していることを示す指数である。この値は、伝搬パラメータと伝搬状況のずれを示すものであるが、この値が0.3(点線で図示)を超える付近で特性が大幅に20劣化する。

図73、図74は通信品質をビットエラーレート(BER)で表したものであり、通信変化の多様性を鑑み、8通りのフェージングパターンにおける通信品質を示したものである。図73では指数が0.25付近の通信状態を示しており、図74では指数0.35付近の通信状態を示している。図73では全て25の通信でBERが0.01以下まで落ちているのに対して、図74では、ほとんどの通信でBERが0.01以上に留まっている。BERが0.01以下である場合は、誤り訂正で情報の復元が可能であることを考えると、指数が0.

3以下であることが本発明の秘匿通信の大きな目安となる。

図72に示した f_d はフェージングピッチを表しており、次式で与えられる。

$$f_d = (S_{max}/C) * F_c / F_{baud} \quad (37)$$

ここで、 S_{max} は最大移動速度、 C は光速、 F_c はキャリア周波数、 F_{baud} はシンボルレート周波数である。こうして求められた値を $f_d = 1/n$ とおくと、図より分るとおり凡そ $n/4 \sim n/3$ （シンボル時間）付近で0.3を超えていることが分る。即ち、安定した通信を行うためには $T_{rep1y} < n/4$ （シンボル時間）を満たす必要がある。ここで無線LANの規格を考えてみる。通信中の最大移動速度を30km/h、キャリア周波数を2.45GHzとすると、式36から T_{rep1y} を満足するための値が求められる。

（ f_d と T_{rep1y} とが F_{baud} によって規定されるため、 F_{baud} は相殺される）

$$T_{rep1y} = C / S_{max} / F_c / 4 \quad (38)$$

上記条件を代入すると、 T_{rep1y} が約3.5ms以下である場合に高い通信品質での通信が可能になる。

このように T_{rep1y} の値に制限があるため、同一周波数帯を用いて複信を行うTDD（Time Division Duplex）通信において、 T_{access} 内に他の通信端末からのアクセスを禁止することが効果的である。即ち T_{access} を T_{rep1y} よりも大きな値（たとえば10ms）に設定しておき、この期間は秘匿通信をおこなう端末同士のみが通信リソースを占有するように上位層が制御することが考えられる。

また、伝送する情報が多い場合、手順(1.3)、(1.4)を繰り返すことで、多くの情報伝送にも対応できる。この場合、先に述べた T_{access} も通信料に対応して長く確保することが望ましい。

次に、セキュア情報を要求する場合の手順について図62を用いて説明する。

(O) 初期化

前述の初期化と同一の作業を行う。

(2) セキュア情報受信

(2. 0) 通信端末Aのアプリケーションが上位層にセキュア情報受信の要求を出力する。

(2. 1) 通信端末Bの上位層はセキュア情報受信要求を受けると、物理層
5 に対してセキュア受信コマンドを発行する。

(2. 2) 通信端末Bの物理層では、セキュア受信コマンドを受信すると、
通信タイミングに従ってセキュア通信要求を伝搬推定用信号とともに通信端
末Bへ送信する。

(2. 3) 通信端末Bの物理層では、セキュア通信要求を受信すると伝搬推
10 定用信号から伝搬を推定し、伝搬パラメータを算出する。同時に上位層に対し
て情報要求コマンドを発行する。(物理層で管理された情報であれば上位層へ
のコマンド発行は行わず(2. 4) (2. 5) は不要。一方上位層で管理された
情報であれば (2. 4) は不要。)

(2. 4) 通信端末Bの上位層では、物理層からの情報要求コマンドを受け
15 てアプリケーションから情報を入手する。

(2. 5) 通信端末Bの上位層では、セットした情報とともに情報応答コマ
ンドを物理層に対して発行する。

(2. 6) 通信端末Bの物理層では、(2. 4) で推定した伝搬パラメータ
を用いて、入手した情報を秘匿通信方法により通信端末Aへ送信する。

20 (2. 7) 通信端末Aの物理層では、秘匿通信方法を用いて伝送されたセキ
ュア情報を受信・復調し、上位層へ出力する。

(2. 8) 通信端末Aの上位層は物理層から出力されたセキュア情報を、ア
プリケーションへ出力する。

以上の一連の動作により、通信端末Aのアプリケーションが通信端末Bに対
25 してセキュア情報を要求し、通信端末Bから通信端末Aに対してセキュア情報
を伝送することが可能になる。本手順に従うことで、セキュア情報を最も簡単
な手順で受信することが可能である。

以上の動作において、物理層における実際の通信信号について図65を用いて説明する。図中で網掛けされた部分は、通信端末Aから通信端末Bへの信号、他は通信端末Bから通信端末Aへの信号を示している。

セキュア通信要求が伝搬用推定信号とともに発行されると(2.2)、所定の間隔(T_{guard})後、この伝搬用推定信号を用いて算出した伝搬パラメータに基づき、セキュア通信が実行される(2.6)。

時間の説明は図64と同様であるため省略する。

先に述べたとおり、 T_{replay} の時間に制約がある場合、(2.3)による情報がすぐに求められない場合が考えられる。この場合に有効な通信手順について図63を用いて説明する。

(0) 初期化

前述の初期化と同一の作業を行う。

(3) セキュア情報受信

(3.0) 通信端末Aのアプリケーションが上位層にセキュア情報受信の要求を出力する。

(3.1) 通信端末Bの上位層はセキュア情報受信要求を受けると、物理層に対してセキュア受信コマンドを発行する。

(3.2) 通信端末Bの物理層では、セキュア受信コマンドを受信すると、通信タイミングに従って情報準備要求を通信端末Bへ送信する。

(3.3) 通信端末Bの物理層では、情報準備要求を受信すると、上位層に対して情報要求コマンドを発行する。(物理層で管理された情報であれば上位層へのコマンド発行は行わず(3.4)(3.5)は不要。一方上位層で管理された情報であれば(3.4)は不要。)

(3.4) 通信端末Bの上位層では、物理層からの情報要求コマンドを受け取てアプリケーションから情報を入手する。

(3.5) 通信端末Bの上位層では、セットした情報とともに情報応答コマンドを物理層に対して発行する。

(3. 6) 通信端末Bの物理層では、情報がセットされたことを情報応答コマンドで通知されると、通信端末Aに対して情報準備完了を通知する。

(3. 7) 通信端末Aの物理層では、通信端末Bからの情報準備完了通知を受信すると、通信タイミングに従ってセキュア通信要求を伝搬推定用信号とともに通信端末Bへ送信する。
5

(3. 8) 通信端末Bの物理層では、セキュア通信要求を受信すると伝搬推定用信号から伝搬を推定し、伝搬パラメータを算出する。次に推定した伝搬パラメータを用いて、入手した情報を秘匿通信方法により通信端末Aへ送信する。

(3. 9) 通信端末Aの物理層では、秘匿通信方法を用いて伝送されたセキュア情報を受信・復調し、上位層へ出力する。
10

(3. 10) 通信端末Aの上位層は物理層から出力されたセキュア情報を、アプリケーションへ出力する。

以上の動作において、物理層における実際の通信信号は前述図65の説明と同一であるので省略する。

15 以上の動作により、アプリケーションが特に通信状態を意識することなく秘匿通信を行うことが可能であるが、アプリケーションによっては特定の情報を秘匿通信で授受したり、受けた情報が秘匿通信されているかの情報が必要な場合もある。この様な場合、図60に示されているように上位層4750での処理において例えば(1. 0)、(2. 0)、(3. 0)、(1. 6)、(2. 20 8)、(3. 10)などのステップでアプリケーションと情報を授受する際に、情報の属性として秘匿通信を用いた事を示すフラグを付しておくことで、アプリケーションがより柔軟な処理が出来ると言った特長を有する。

この様に、本実施の形態27を用いることで、上位層から物理層での効率的な秘匿通信の制御を可能にし、安定した通信プロトコルを提供する。

25 (実施の形態28)

本実施の形態28は、実施の形態17、18で説明した発明をさらに拡張して、送信端末が有する送信アンテナの本数を見かけ上多くすることを可能にし、

秘匿性を向上させることを特徴とする。

本実施の形態で用いる通信システムを図77に示す。

通信端末A7750と通信端末B7751はチャネル7752を介して通信を行っている。また、通信端末A7750は1つの送受信アンテナ素子を、

- 5 通信端末Bは4つの送受信アンテナ素子を有している。

まず、通信端末A7750について説明する。

変調部7701はデータを入力し、それを変調した変調信号を出力する。

バッファ7702は変調信号を入力・保持したバッファド変調信号をチャネル合成部7703へ出力する。

- 10 チャネル合成部7703は変調信号にチャネルパラメータを用いて合成し、送信信号を送信部7704へ出力する。

送信部7704は送信信号を周波数変換、電力増幅し、送信RF信号をアンテナ7705へ出力する。

- 15 アンテナ7705は送信RF信号を放射し、受信した受信RF信号を受信部7706へ出力する。

受信部7706はアンテナ7705から入力した受信RF信号からベースバンド信号をチャネル推定部7707へ出力する。

チャネル推定部7707は受信部7706から入力したベースバンド信号からチャネル7752の特性を推定し、推定チャネル情報を出力する。

- 20 チャネル解析部7708は推定チャネル情報を入力し、所定の解析方法を用いてチャネルパラメータを算出し、出力する。

次に、通信端末B7751について説明する。

アンテナ7709は送信RF信号を入力しこれを放射すると共に、受信した受信RF信号を送信部7710へ出力する。

- 25 受信部7710は受信RF信号からベースバンド信号へ変換しバッファ7711へ出力する。

バッファ7711はベースバンド信号を一時保持し、所定時間だけずらした

信号を選択合成部に出力する。

選択合成部 7712 は時間差のついた信号を合成し、合成信号を出力する。

復調部 7713 は合成信号を入力し、これを復調してデータを得る。

参照信号格納部 7714 はチャネル 7752 を推定するための参照信号を

5 格納し出力する。

アンテナ選択部 7715 は参照信号を入力し、これを選択されたアンテナに送信信号として出力する。

送信部 7716 は、送信信号を入力し送信 R.F. 信号を対応するアンテナ素子 7709 へ出力する。

10 ここで、通信伝搬路のチャネルを h_1 、 h_2 、 h_3 、 h_4 で構成されるチャネルマトリクス H として考える。通信端末 A 7750 が通信端末 B 7751 からの参照信号を用いて伝搬を推定するが、このとき通信端末 A 7750 が通信端末 B 7751 の各アンテナとの係数を測定できるように、夫々のアンテナから直交した信号を出力する。ここでは、その代表として時分割で参照信号を出力するものとする。こうすることで、通信端末 A は h_1 、 h_2 、 h_3 、 h_4 を測定することが可能になる。

則ち、参照信号格納部 7714 から出力された参照信号をアンテナ選択部 7715 が順次出力するアンテナを切り換える。この様にして出力された送信信号は送信部 7716 で増幅され対応するアンテナから放射される。

20 通信端末 A では、アンテナ 7705 で上記参照信号を受信すると受信 R.F. 信号が受信部 7706 へ入力され順次ベースバンド信号へと変換される。チャネル推定部 7707 ではベースバンド信号を入力し参照信号を用いてチャネルの推定が行われ、チャネル情報を出力する。チャネル情報はチャネル解析部 7708 に入力され、その解析が行われる。ここでは実施の形態 18 で説明した特異値分解を用いて説明する。特異値分解で得られた特異値ベクトル V は、特異値が非 0 の特異ベクトルと特異値が 0 のゼロベクトルとに分離できる。ここで各ベクトルを $v_1 \sim v_4$ 、 v_1 を特異ベクトル、 $v_2 \sim v_4$ をゼロベクトル、

特異値を入とする。またベクトル要素を $v_n = (v_{n1} \sim v_{n4})$ ($n=1 \dots 4$) と定義する。これら特異ベクトルとゼロベクトルをチャネルパラメータとして出力する。

変調部 7701 は 4 系列のデータを入力し、所定の変調方式に則り変調信号 5 を 4 系列生成し出力する。この変調信号を $d_1 \sim d_4$ とし、 d_1 を通信用変調信号、 $d_2 \sim d_4$ を疑似変調信号とする。バッファ部 7702 は、4 系列の変調信号を入力しこれを保持する。バッファ部 7702 は 4 タイムスロット分同一の信号を保持し続ける。

最初のタイムスロットにおいて、チャネル合成部 7703 は 4 系列の変調信号 10 とチャネルパラメータを入力し、以下の演算を行う。

$$DS_1 = \sum (v_{n1} \cdot d_n) \quad (39)$$

(n は Σ 変数とする、以下同様)

この様にして得られた送信信号を送信部 7704 へ出力する。

以下同様に k 番目タイムスロットにおいて、チャネル合成部 7703 は変調 15 信号 $d_1 \sim 4$ を入力し以下の演算を行う。

$$DS_k = \sum (v_{nk} \cdot d_n) \quad (40)$$

こうして出力された 4 タイムスロット分の送信信号は、伝搬路 7752 を介して通信端末 B 7751 で受信される。通信端末 B 7751 の受信処理の詳細を図 78 に示す。各アンテナで受信した受信 RF 信号は対応する受信部 771 20 0 によってベースバンド信号に変換され出力される。ベースバンド信号はバッ ファ部 7711 によって一時保持される。ここでは 4 タイムスロット分 \times 4 アンテナ系列で 16 のバッファを表記してある。上記動作によって 4 タイムスロット分、バッファ部 7711 で蓄えられた信号を夫々 $S_{rx11} \sim S_{rx44}$ とする。この信号は、チャネル要素 $h_1 \sim h_4$ 、チャネルパラメータ要素 $v_1 \sim v_4$ 25 4、変調信号 $S_t_1 \sim 4$ を用いて以下のように表現できる。

$$S_{rxjk} = h_j \cdot \sum (v_{nk} \cdot d_n) \quad (41)$$

ここで、図 68 に図示したように、 $S_{rj} = S_{rxjk}$ ($j=k, j=1 \dots 4$)

4) の信号について注目すると次式が得られる。

$$S_r j = h_j \cdot \Sigma (v_n j \cdot d_n) \quad (42)$$

また、 $\Sigma S_r n$ は行列 H、V、D を用いて次式で与えられる。

ここで D は $[d_1 \ d_2 \ d_3 \ d_4]^T$ である (A^T は A の転置行列)。

5 $\Sigma S_r n = H \cdot V \cdot D = \lambda d_1 \quad (43)$

以上のような操作により、通信端末 A 7750 が送信しようとした変調信号 d_1 が得られ、他の変調信号はキャンセルされることが分かる。復調部 7713 はこうして得られた信号をそのまま復調すれば、データが得られる。

ここで、第 3 者がこれを復調しようとしても他の実施の形態と同様、チャネルパラメータが不明であるため、 d_1 を分離することが出来ず復調できない。
この様にすることで、受信・復調には特別な演算を必要とせず秘匿通信を実現できると言った大きな特長がある。

以上説明したことの通信信号について、図 67、75 を用いて説明する。

図中の網掛けは通信端末 B 7751 から通信端末 A 7750 へ出力される信号を示しており、他は通信端末 A 7750 から通信端末 B 7751 へ出力される信号を示している。

図中に示したように、セキュア通信要求信号と共に、伝搬推定用信号が出力される。本実施の形態では、タイムスロットを通信端末 B 7751 のアンテナ素子数だけ設けて送信するとしたが、前述の通り各アンテナ要素から出力される信号が直交していればこれに限ったものではない。図中に示した P1 ~ P4 は対応するアンテナからそれぞれ出力される既知信号であり、これに基づいて通信端末 A 7750 のチャネル推定部 7707 は伝搬路を推定する。次に、通信端末 A 7750 は、秘匿通信を行う際、4つのタイムスロットを用意して (DS1 ~ DS4) 式 40 で与えられる信号を送信することで、秘匿通信は行われる。

以上の説明に於いて、通信端末 A 7750 におけるアンテナ 7705 の要素数を 1、通信端末 B 7751 におけるアンテナ 7709 の要素数を 4 として説

明したが、これに限ったものではない。本発明は通信端末A 7750の要素数をm、通信端末B 7751の要素数をnとしたとき $m < n$ 場合に、より高度の高い通信方式を提供するものである。mが2以上である場合、nのうちk ($k < m$) であるようなアンテナ選択を行い、他の実施の形態で示したような秘匿通信も可能であるが、本発明はチャネル要素数を最大に取って秘匿通信が行えることから、最も高度な通信保護が為されていると言える。

この様に、本実施の形態28を用いることで、アンテナ要素数 (m) が少ない通信端末がアンテナ要素数 (n) の多い通信端末に対して、最も高度な通信保護を可能とすることが特長であり、特にmが1の場合に大きな効果を発揮する。

上記実施の形態1～28においては、ハードウェアの構成により伝搬環境に応じた秘匿情報を取得することとしたが、これに限らず、プログラム等を用いたソフト上の処理により伝搬環境に応じた秘匿情報を取得するようにしても良い。この場合は、CD-ROM等の記憶媒体に記憶させたプログラム等やネットワークを介して伝送されてきたプログラム等の任意の方式により取得したプログラム等を用いることが可能である。

以上説明したように、本発明によれば、伝搬状態に応じたデータを取り出すことができるので、大きな通信システムの変更をすることなしに高いセキュリティを確保することができる。

本明細書は、2002年2月28日出願の特願2002-054064、2002年5月7日出願の特願2002-132068及び2003年2月25日出願の特願2003-48364に基づくものである。この内容をここに含めておく。

25 産業上の利用可能性

本発明は、ディジタル通信に用いられる技術であって、特にセキュリティに関する技術に用いるに好適である。

請求の範囲

1. 通信相手から送信された信号を用いて伝搬環境を推定する伝搬環境推定手段と、前記伝搬環境推定手段により得られた推定値を用いて第1データを取得する第1データ取得手段と、を具備することを特徴とする通信装置。
5. 2. 前記第1データ取得手段にて取得した前記第1データを用いて受信信号を復号化することにより第2データを取得する復号化手段を具備することを特徴とする請求の範囲1記載の通信装置。
10. 3. 前記伝搬環境推定手段により得られた前記推定値を符号化する符号化手段を具備し、前記第1データ取得手段は、符号化した前記推定値の符号化パターンより前記第1データを取得することを特徴とする請求の範囲1記載の通信装置。
15. 4. チャネル毎に求めた前記推定値をチャネル毎に互いに比較する比較手段を具備し、前記第1データ取得手段は、前記比較手段の比較結果に基づいて前記第1データを取得することを特徴とする請求の範囲1記載の通信装置。
20. 5. 通信相手との間で互いに既知である基準信号を格納する格納手段を具備し、前記伝搬環境推定手段は、前記基準信号と前記信号との相関を求めて前記推定値としての遅延プロファイルを作成し、前記第1データ取得手段は、遅延プロファイルと第1データとが対応付けられた参照テーブルを用い、当該参照テーブルから前記伝搬環境推定手段により作成された遅延プロファイルに対応した第1データを読み出すことで前記第1データを取得することを特徴とする請求の範囲1記載の通信装置。
25. 6. 前記第1データ取得手段は、前記基準信号の自己相関関数成分と前記参照テーブルに記憶されている量子化ベクトルとを畳み込み演算し、前記遅延プロファイルと畳み込み演算した前記量子化ベクトルとを用いてメトリクス演算してベクトルコードを選択することにより前記第1データを取得することを特徴とする請求の範囲5記載の通信装置。
7. 前記第1データ取得手段は、前記伝搬環境推定手段にて作成した前記遅延

プロファイルを直交変換して信号成分を凝縮した後に、当該信号成分を用いて前記第1データを取得することを特徴とする請求の範囲5記載の通信装置。

8. 前記伝搬環境推定手段により得られた前記推定値に基づいて受信信号を等化処理して第2データを取得する等化手段を具備することを特徴とする請求の範囲1記載の通信装置。

9. 第1通信装置は、信号を送信する際の伝搬環境を制御する伝搬環境制御手段と、前記伝搬環境制御手段にて制御した伝搬環境にて前記信号を送信する送信手段とを具備し、前記第2通信装置は、前記第1通信装置から送信された前記信号を受信して当該信号を用いて伝搬環境を推定する第1伝搬環境推定手段と、前記第1伝搬環境推定手段により得られた推定値を用いて第1データを取得する第1データ取得手段と、を具備することを特徴とする通信システム。

10. 前記第1通信装置は、前記第2通信装置から送信された信号を用いて伝搬環境を推定する第2伝搬環境推定手段と、複数のアンテナ素子とを具備し、前記送信手段は、前記第2伝搬環境推定手段により得られた推定値を用いて特定の前記第2通信装置が前記第1データを取得することができるよう前記アンテナ素子毎に送信信号に重み付けして送信することを特徴とする請求の範囲9記載の通信システム。

11. 前記第2通信装置は、前記第1伝搬環境推定手段により得られた前記推定値を用いて第2データを符号化する符号化手段と、前記第2データを変調する変調手段と、前記第2データを送信する送信手段と、を具備することを特徴とする請求の範囲9記載の通信システム。

12. 通信相手から送信された信号を用いて伝搬環境を推定するステップと、推定した伝搬環境の推定値を用いて第1データを取得するステップと、を具備することを特徴とする受信方法。

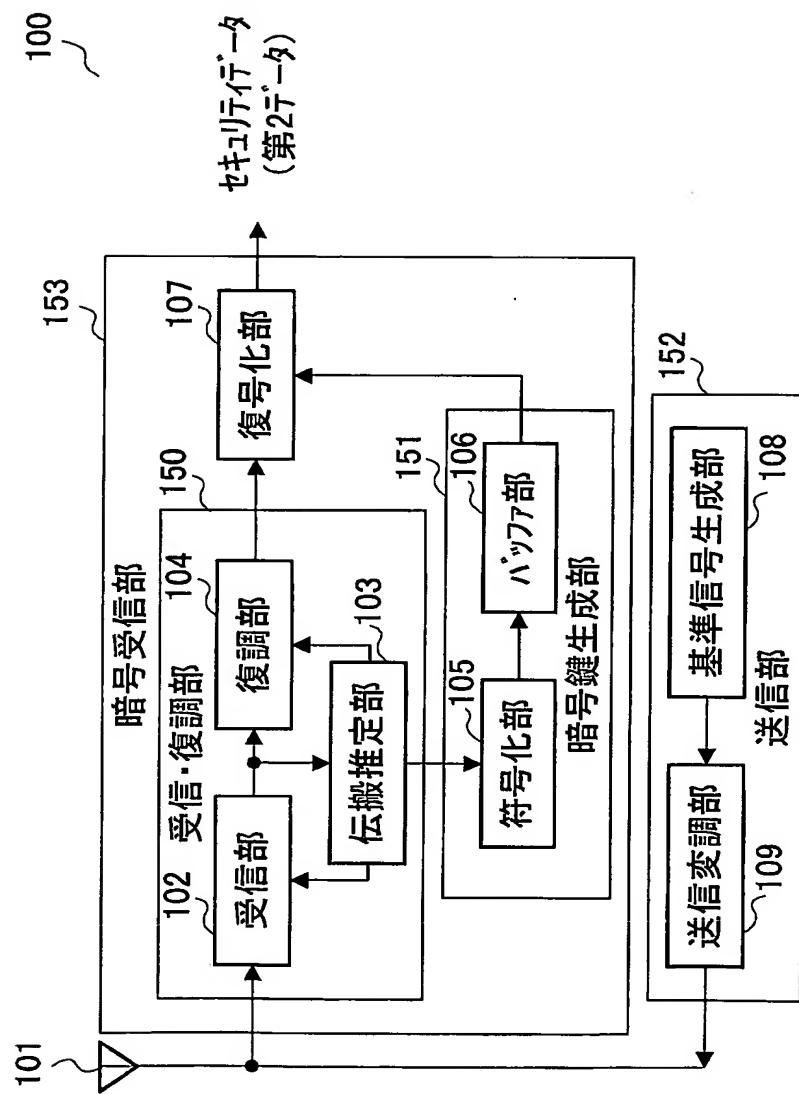


図1

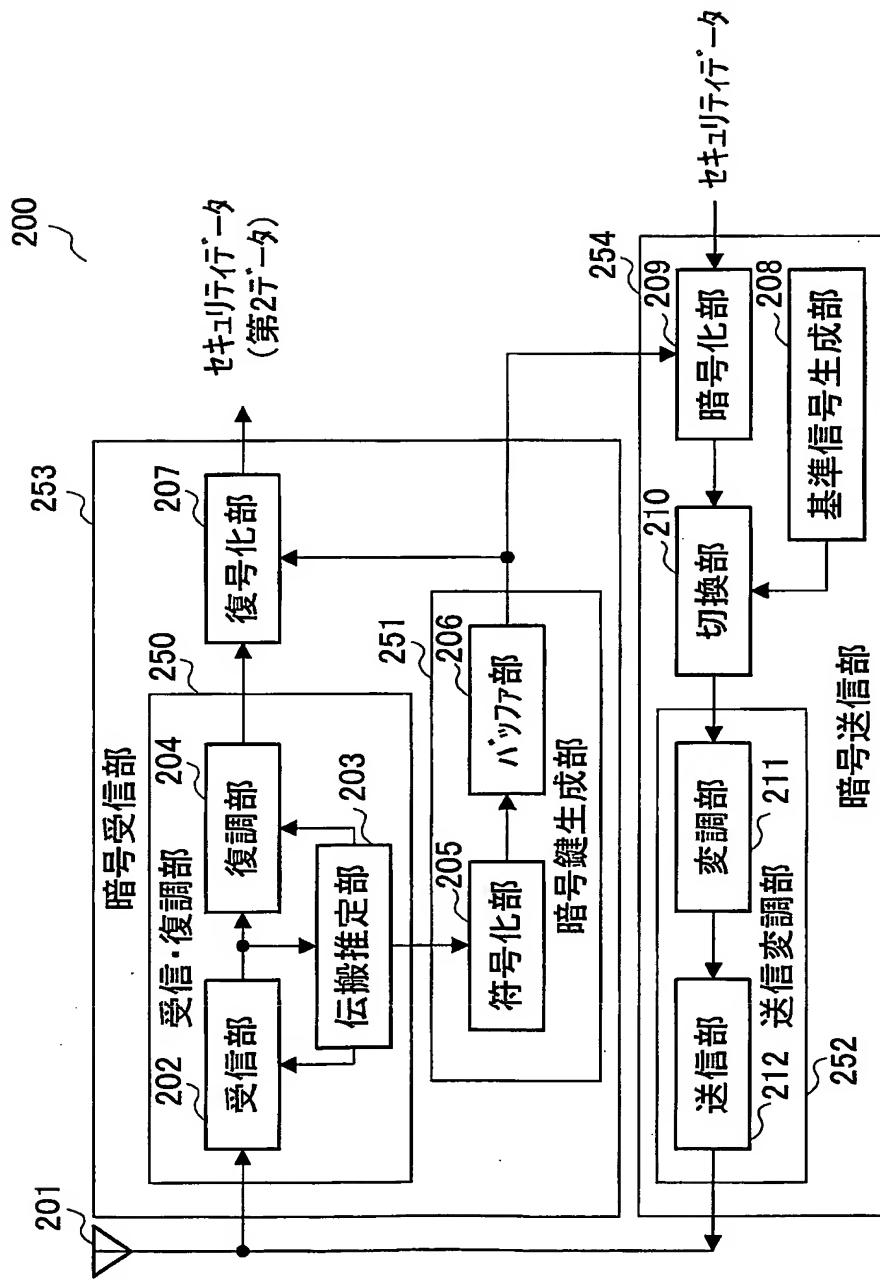


図2

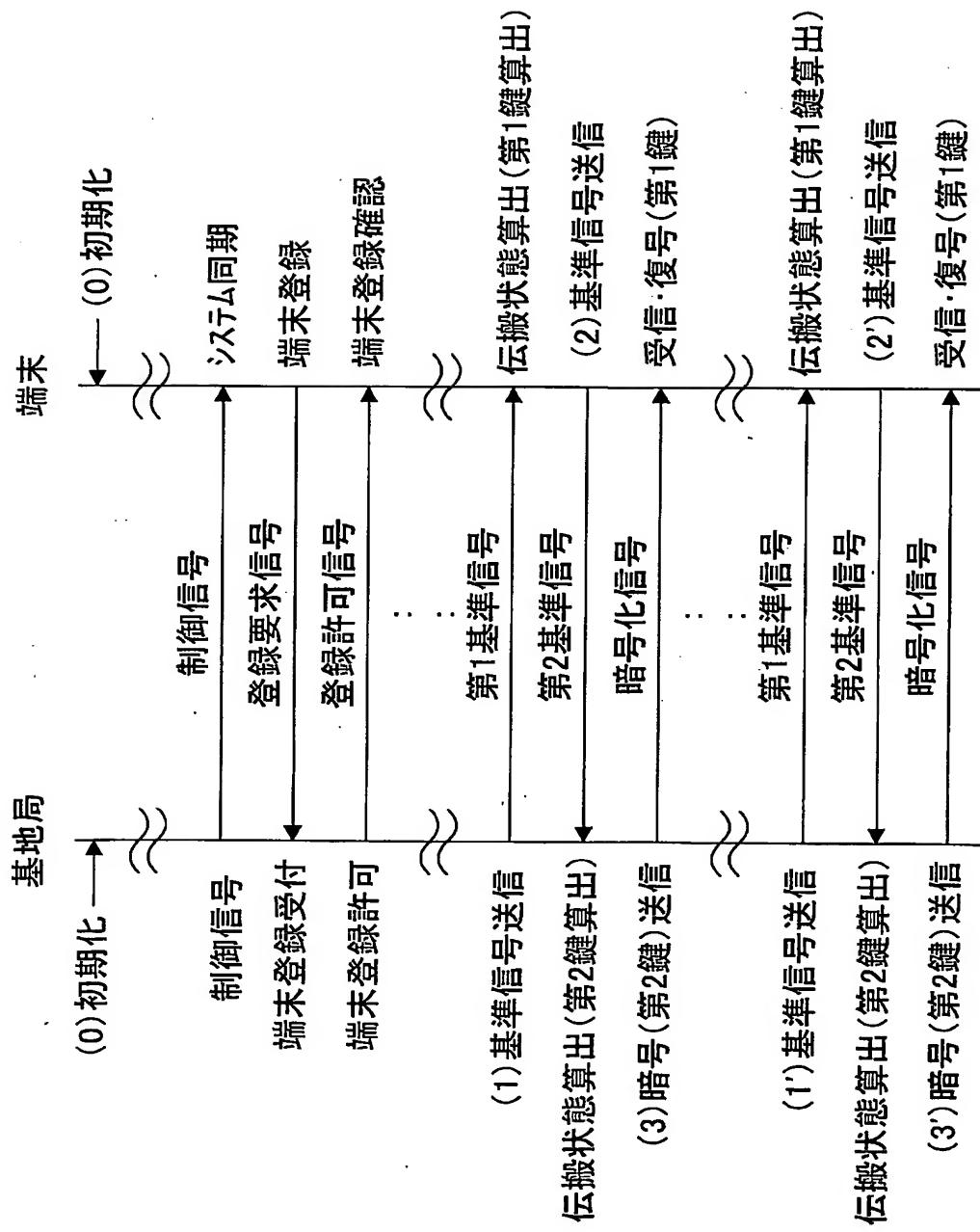


図3

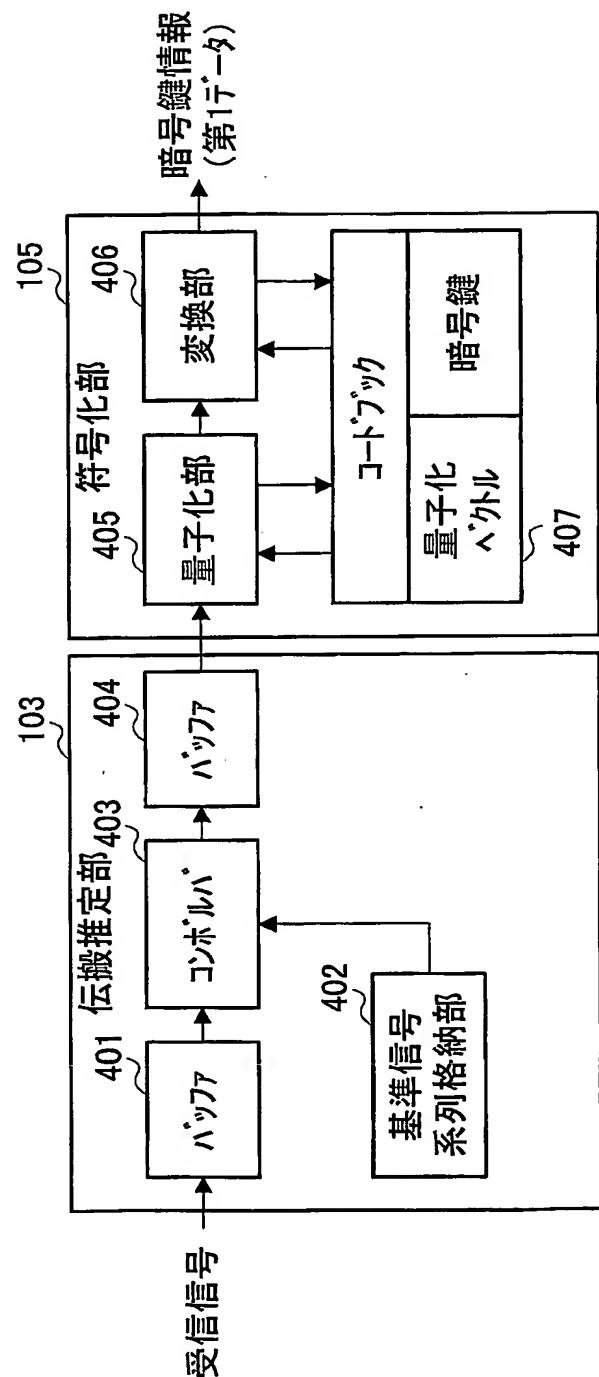


図4

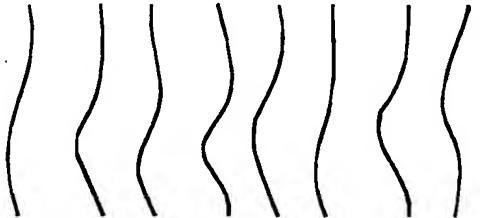
量子化ハカル	暗号鍵
	aAnPoCgk Yncwkopq BemKingT qCTuNvpz RkPoCvvW uCqDGwpo LfUUfEzc IlueGenc

図5

6/78

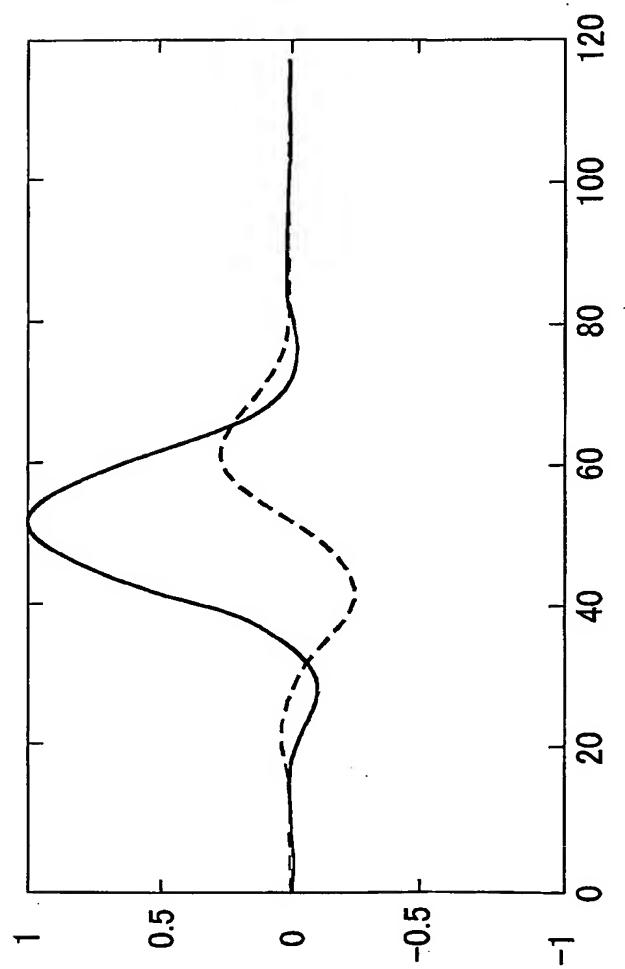


図6

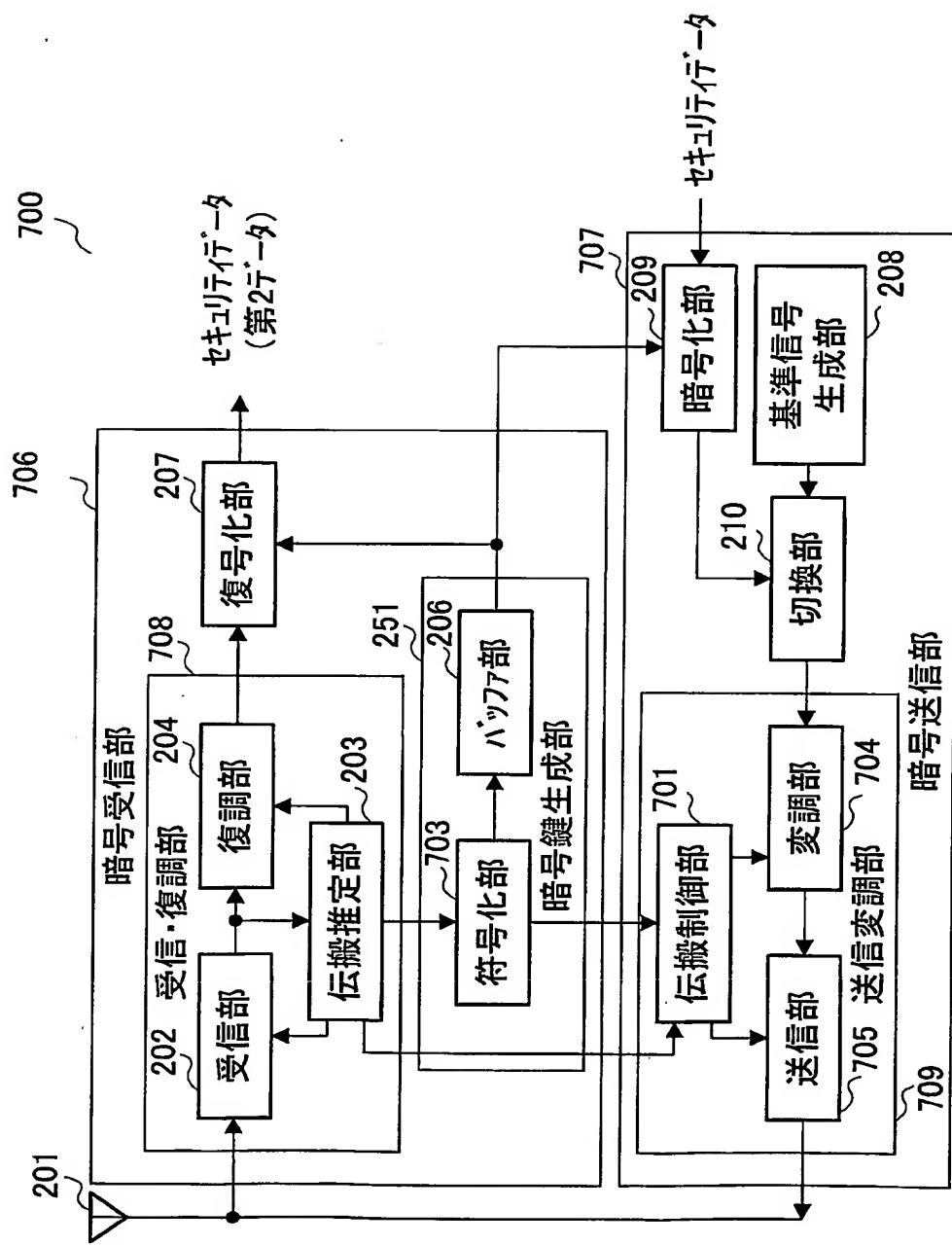


図7

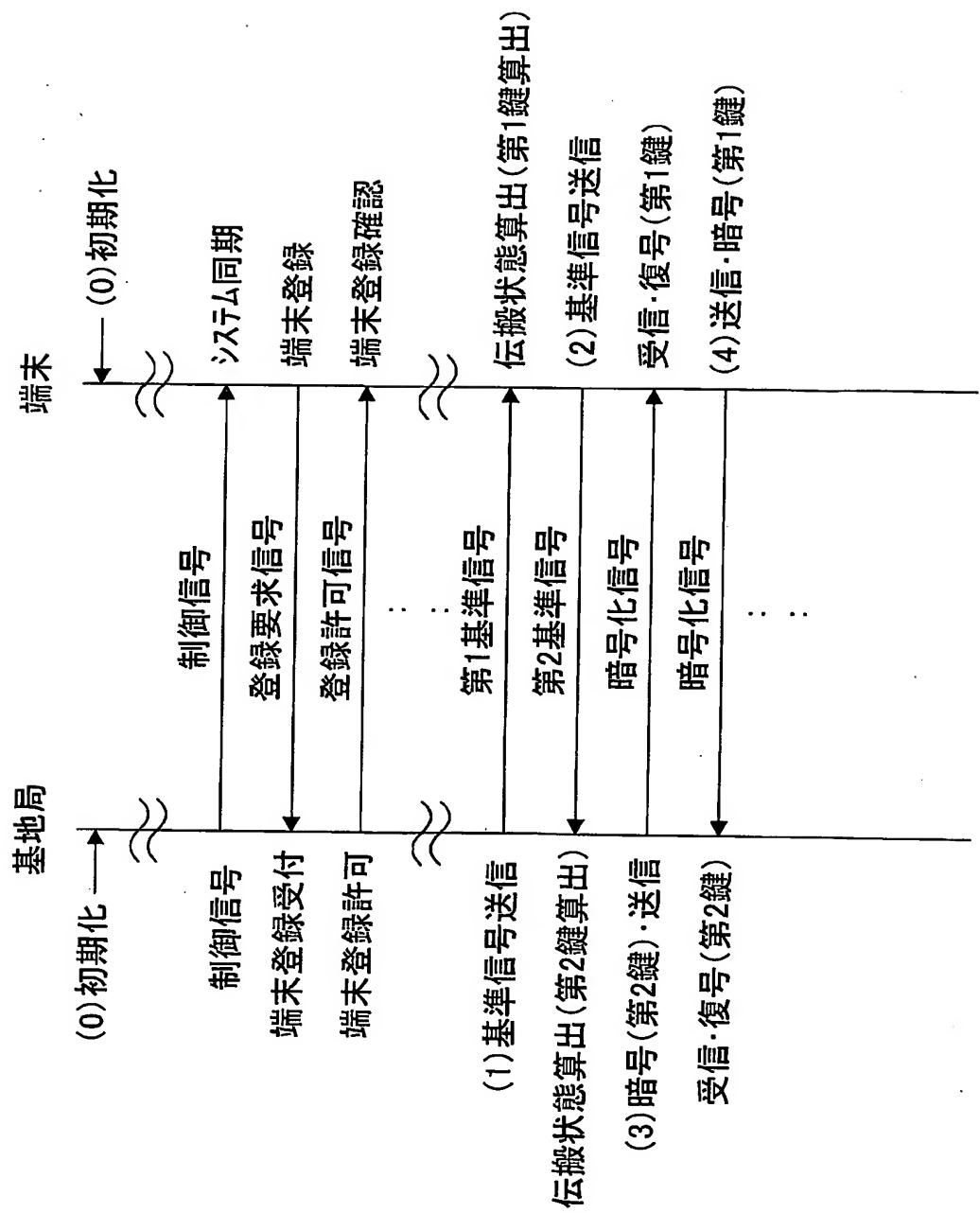


図8

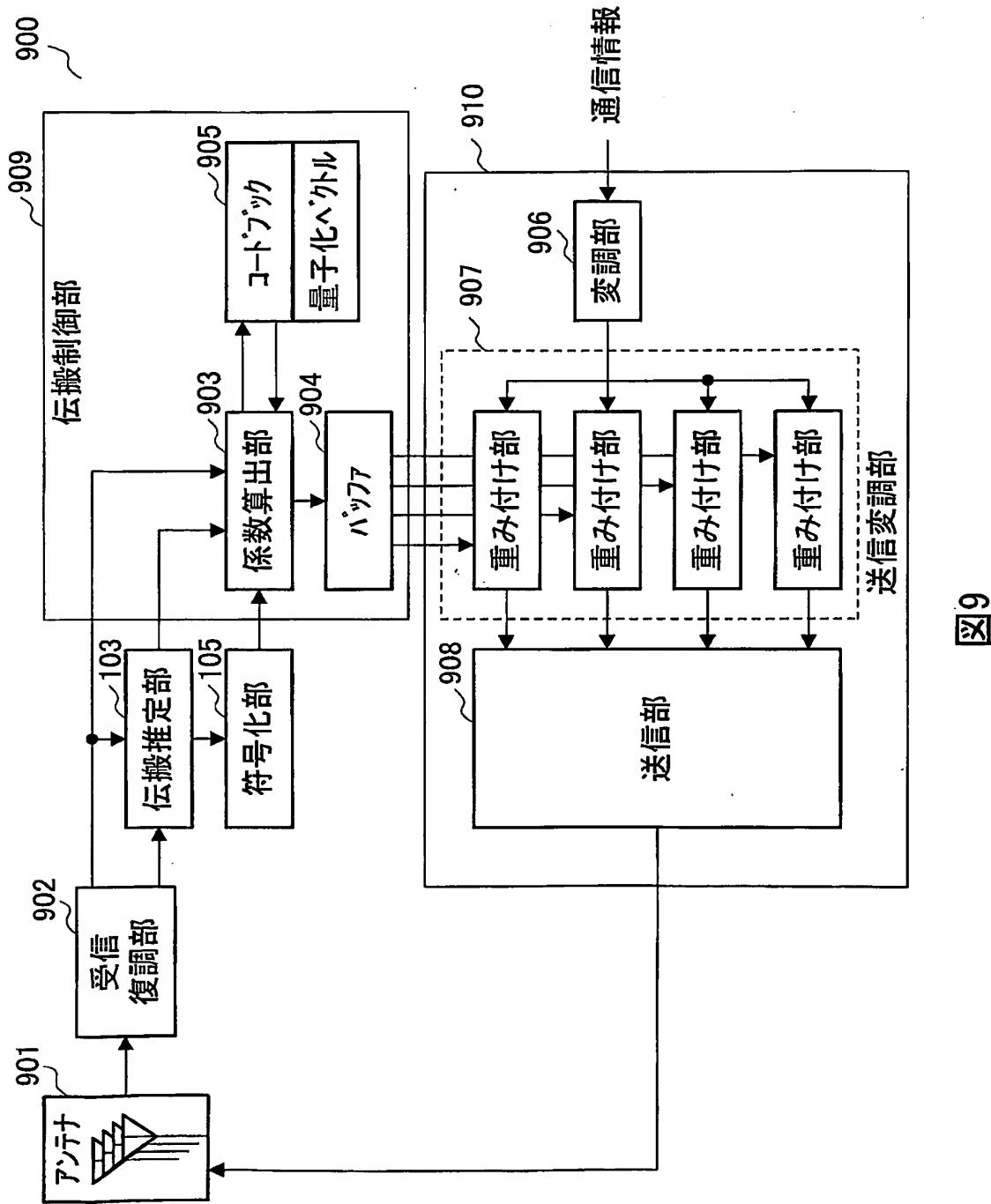


図9

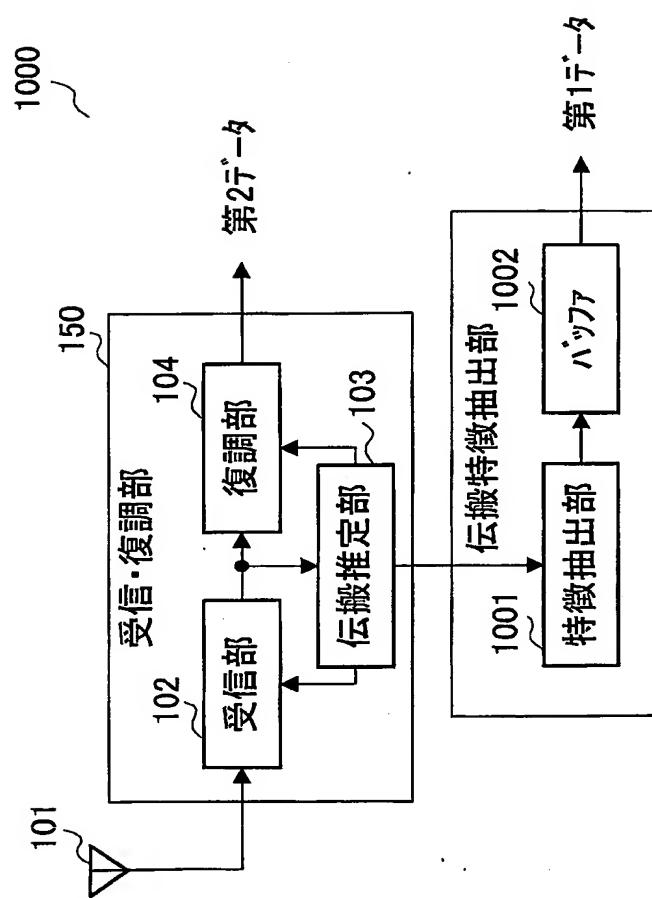


図10

11/78

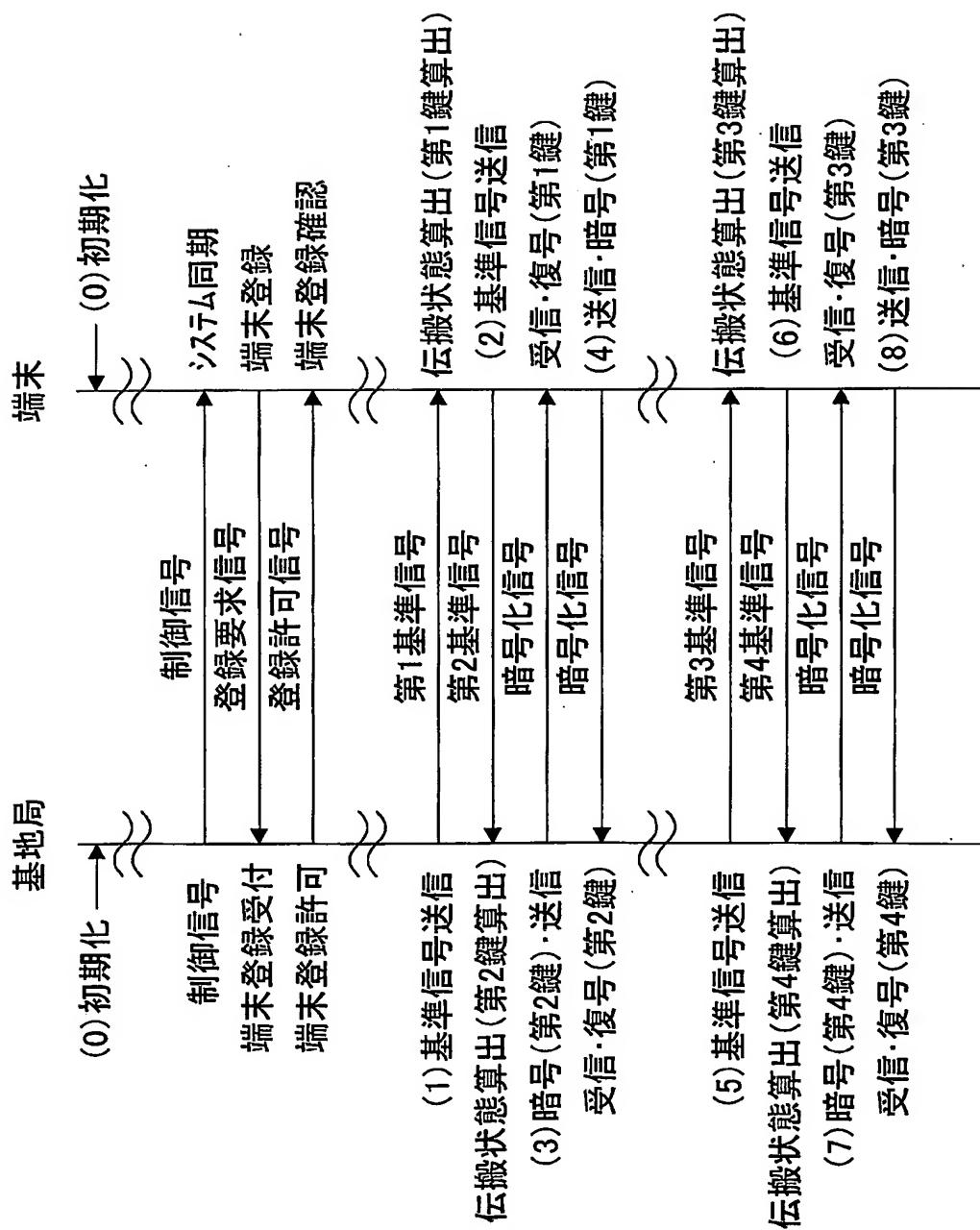
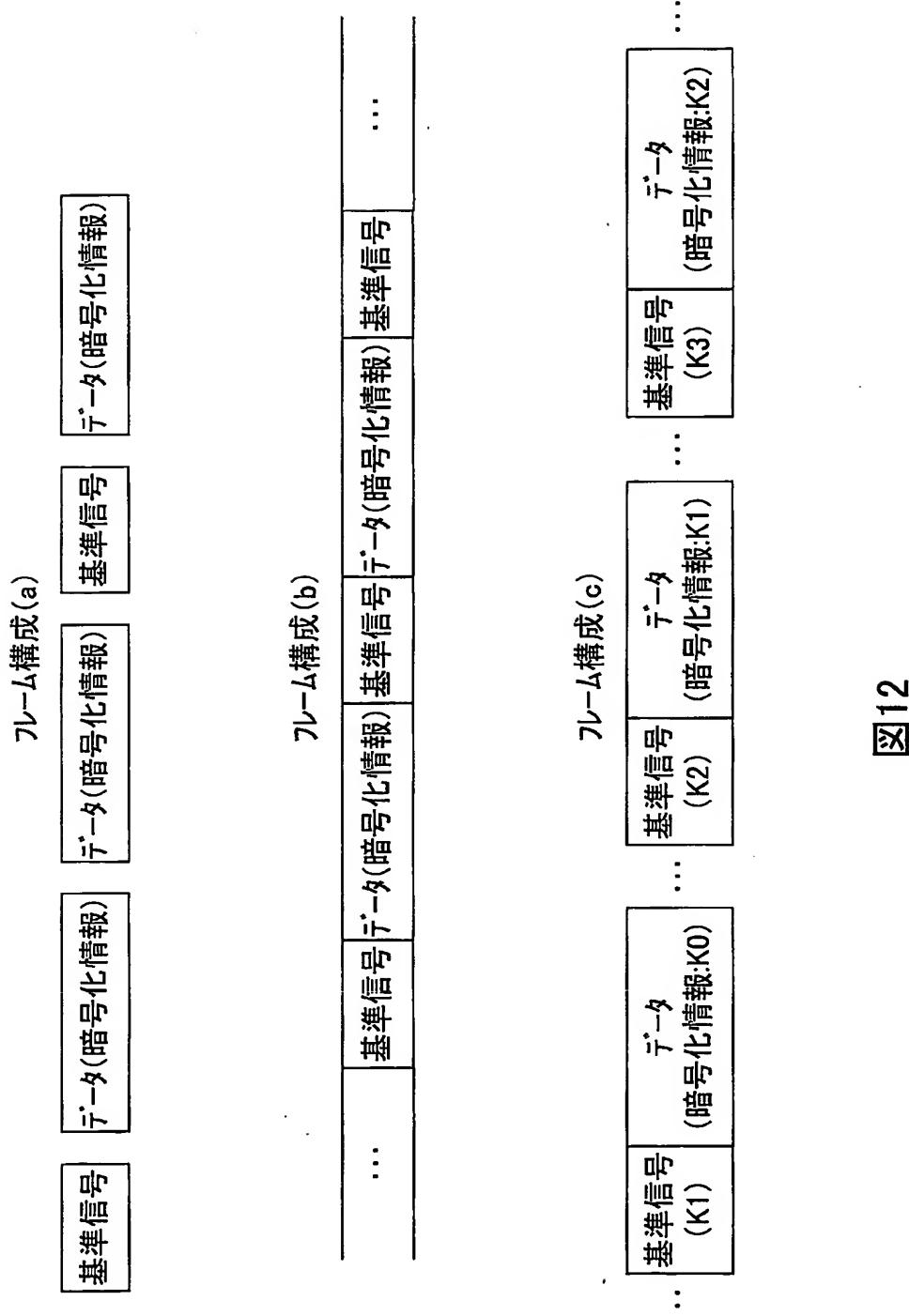


図11

12/78



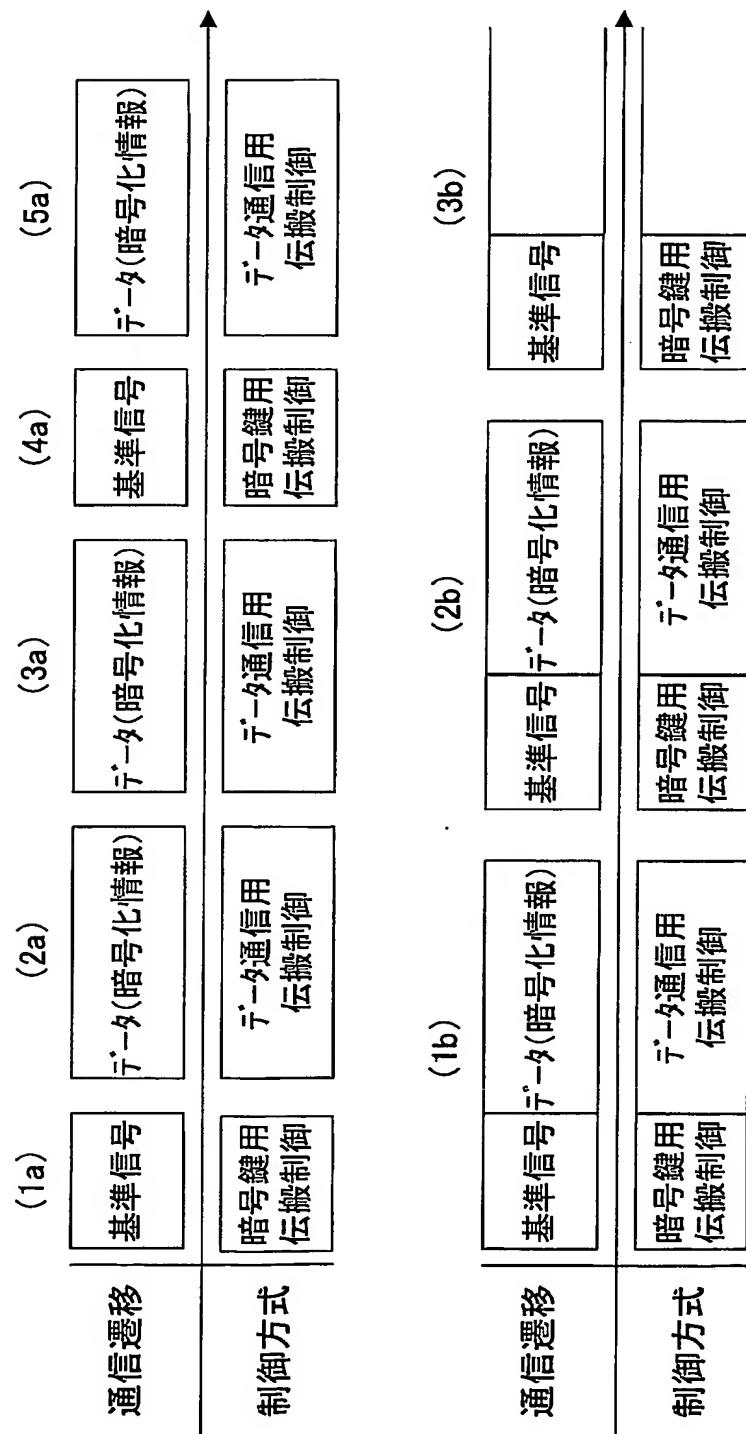


図13

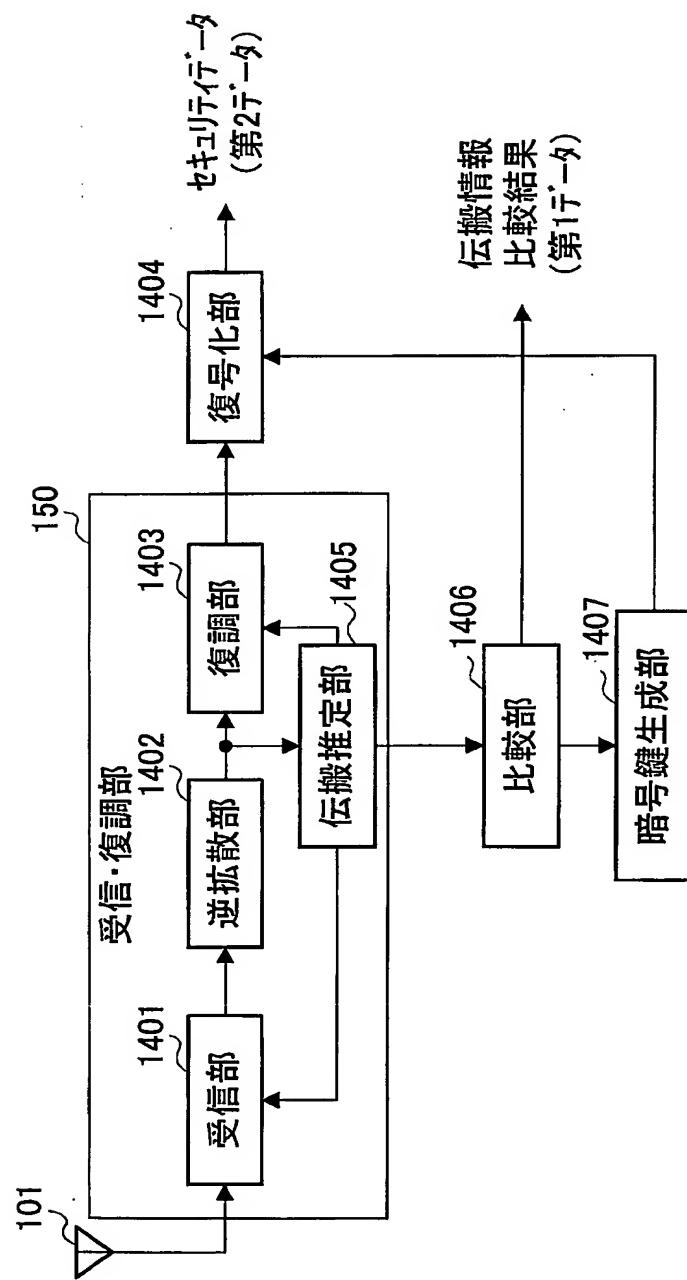


図14

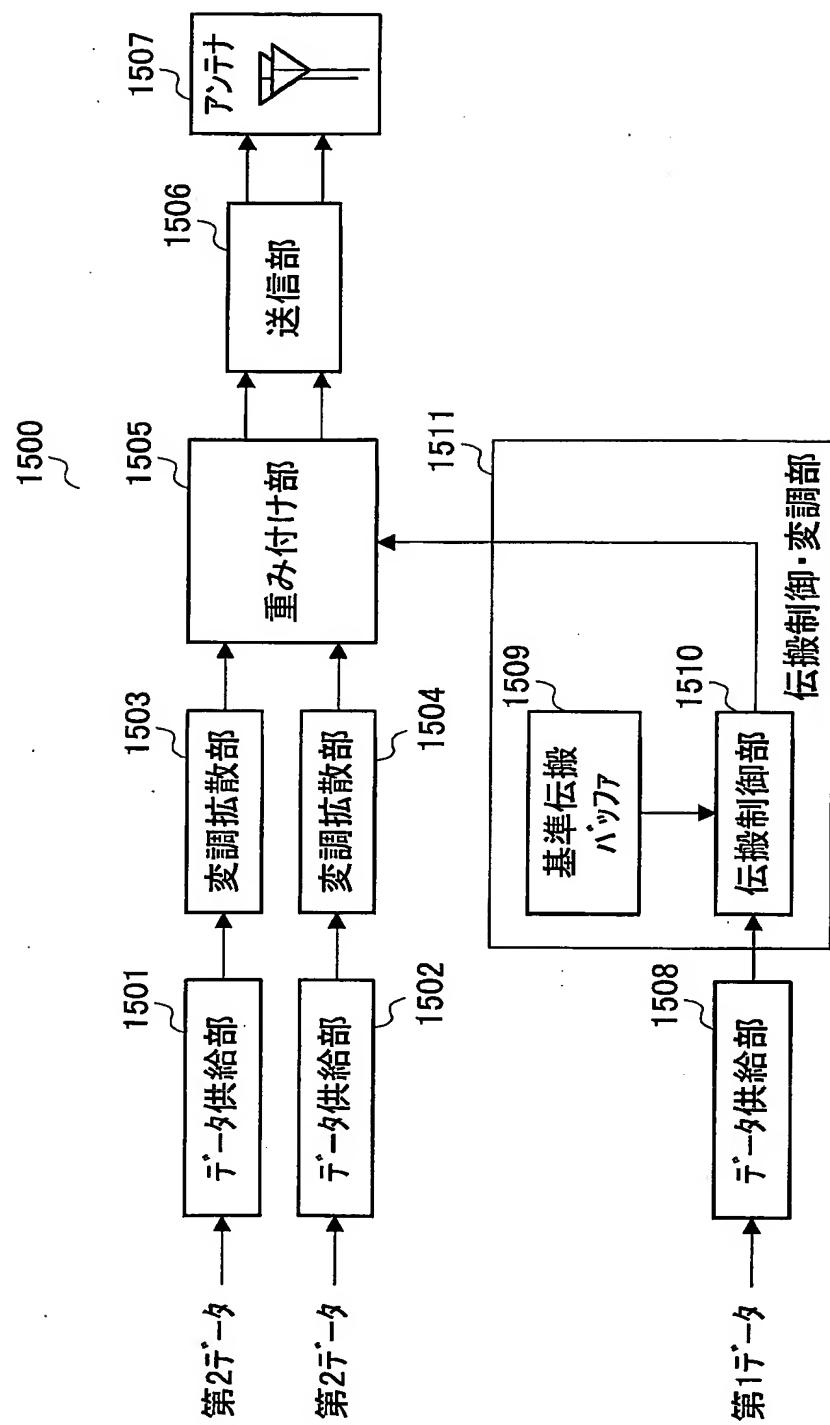


図15

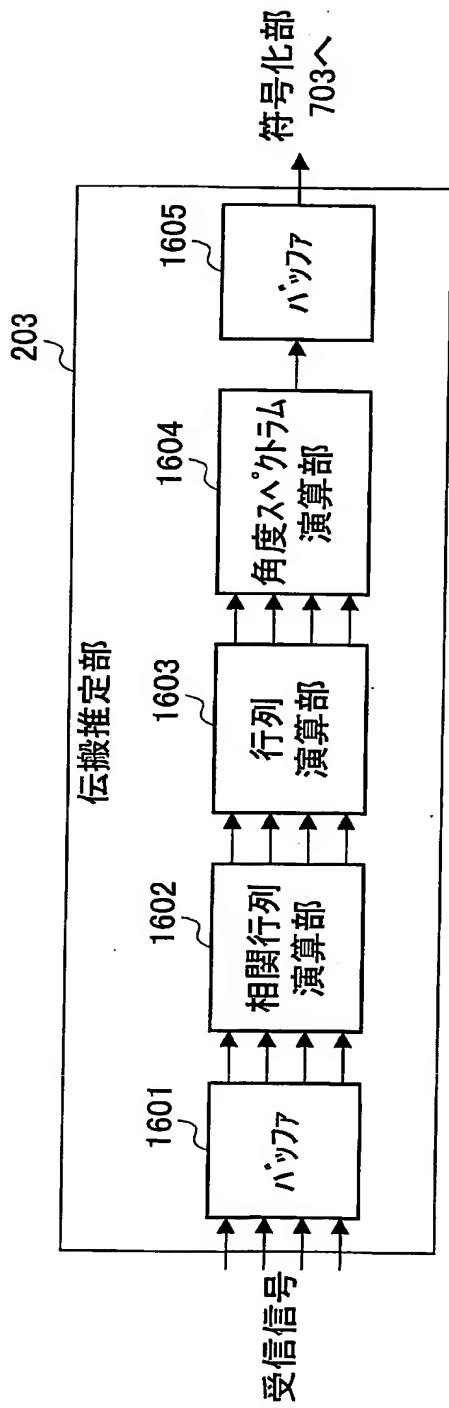


図16

17/78

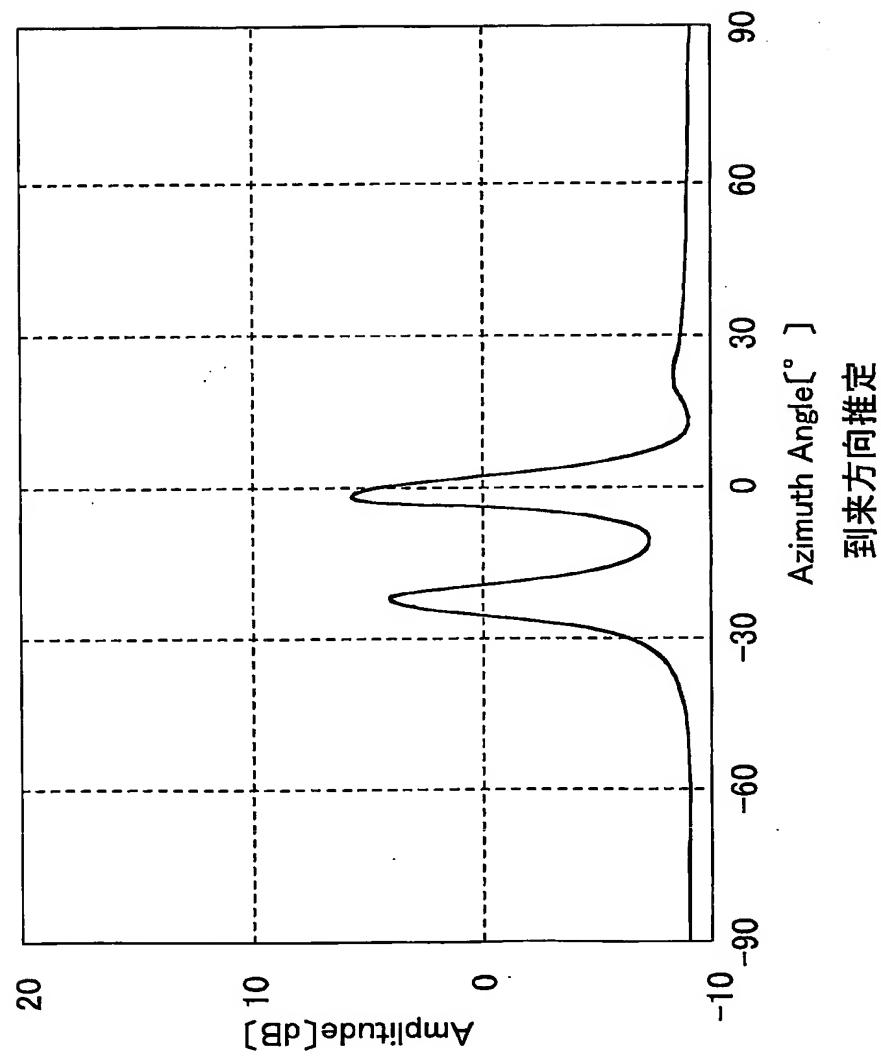


図17

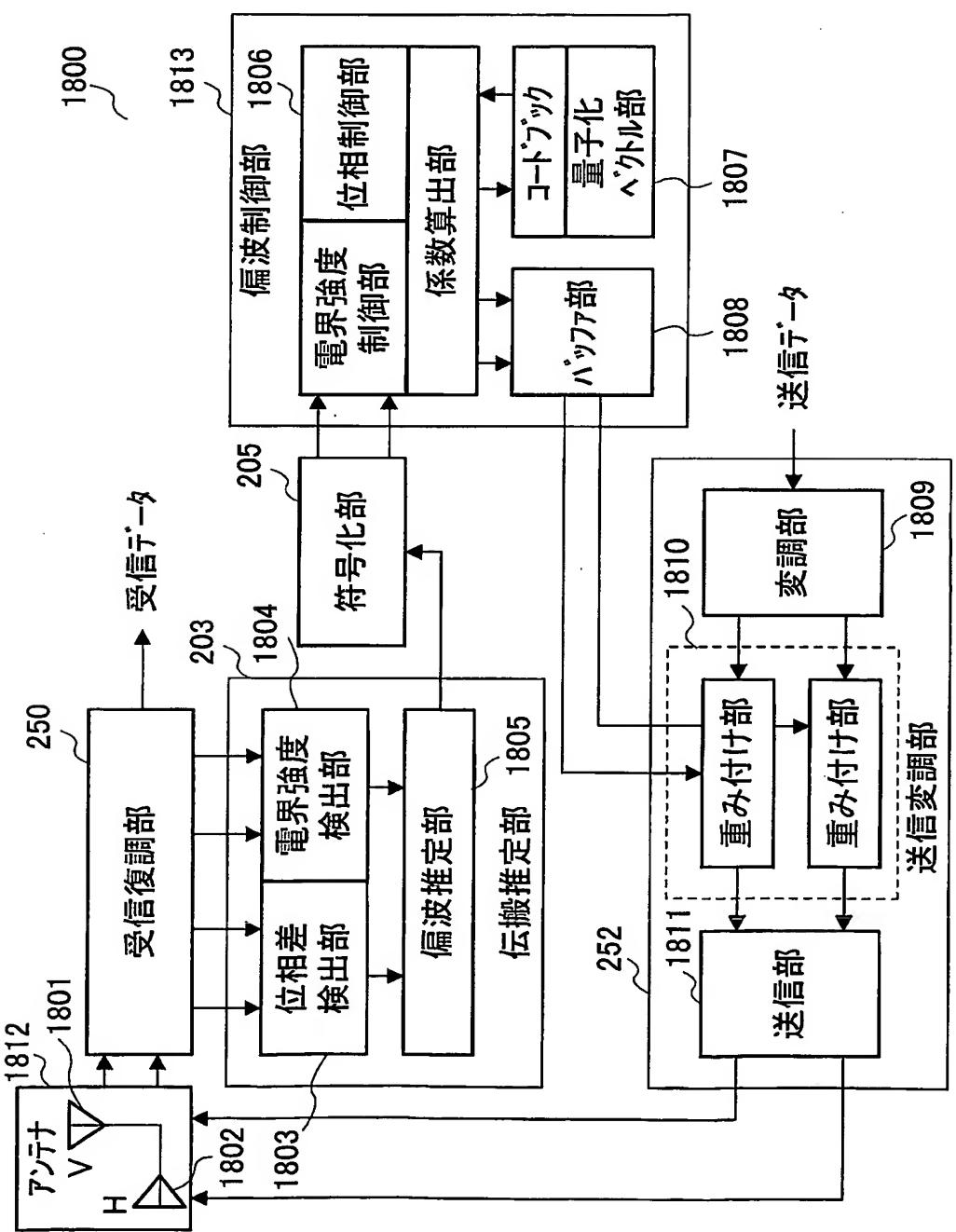


図18

19/78

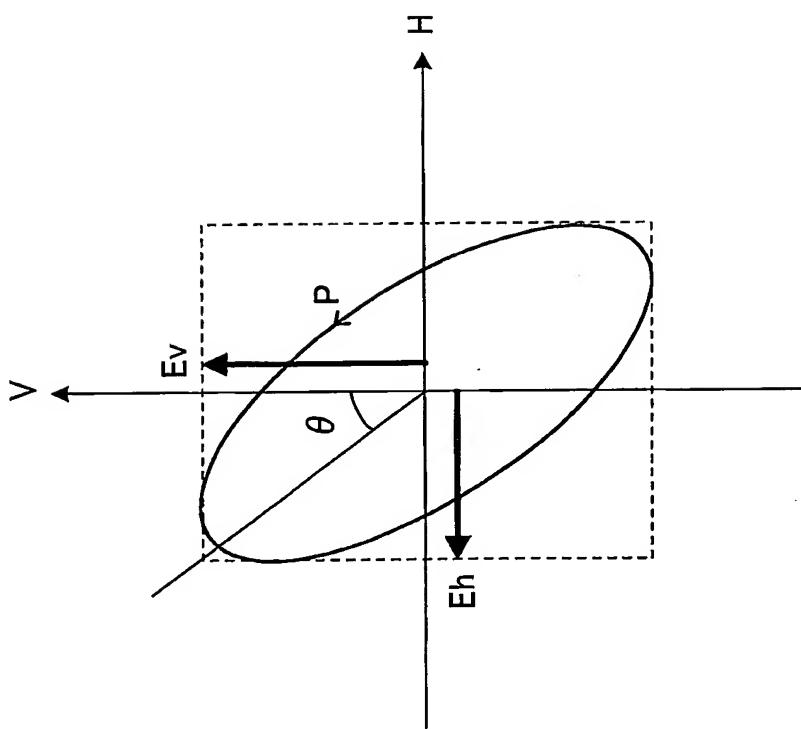


図19

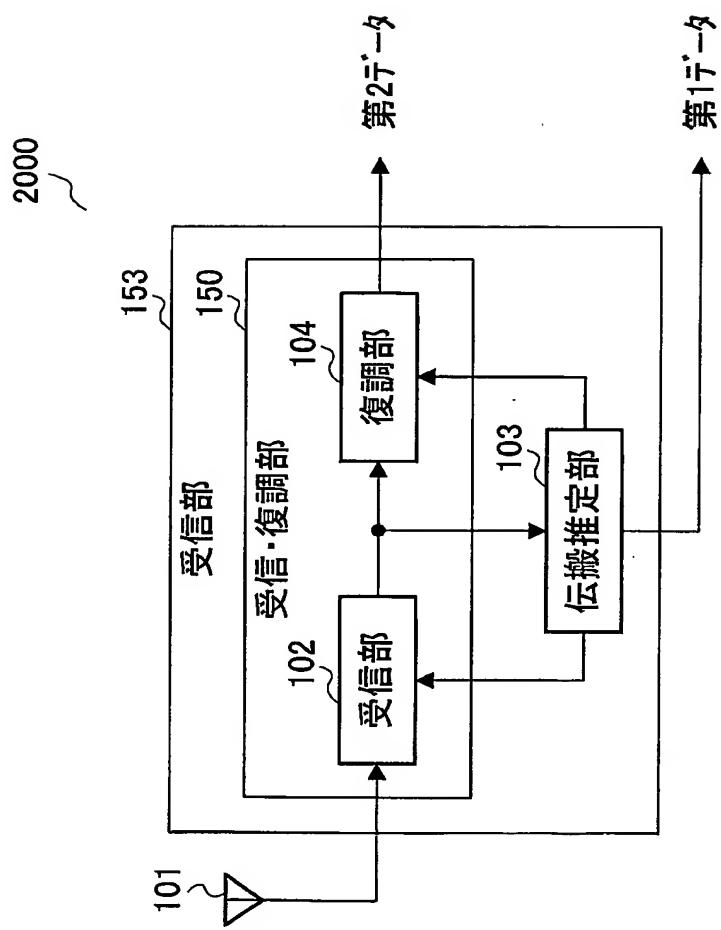


図20

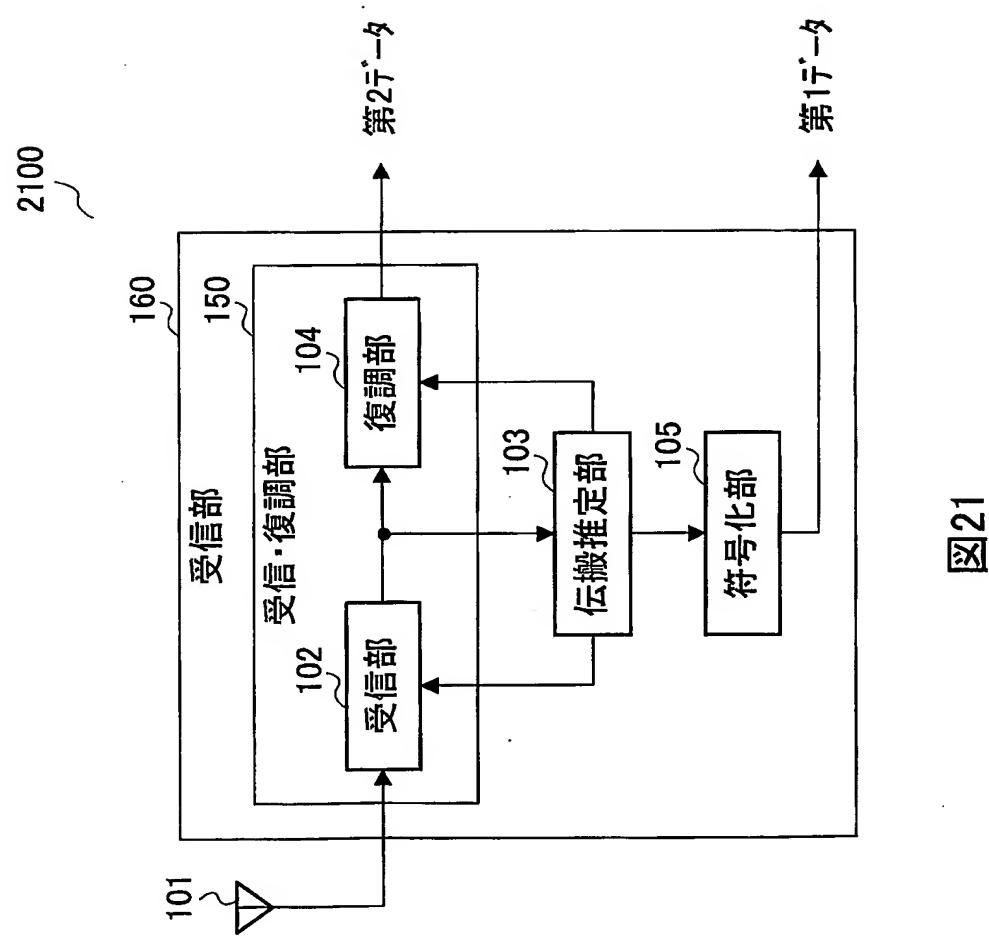


図21

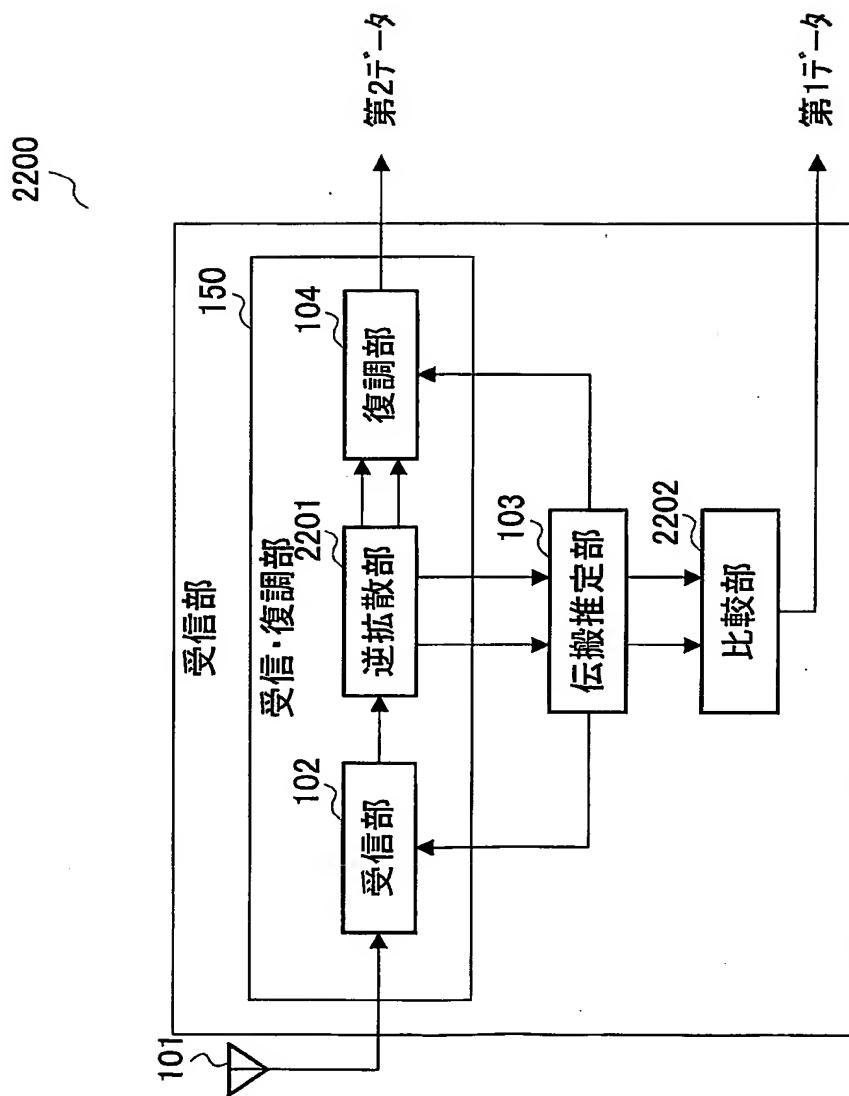


図22

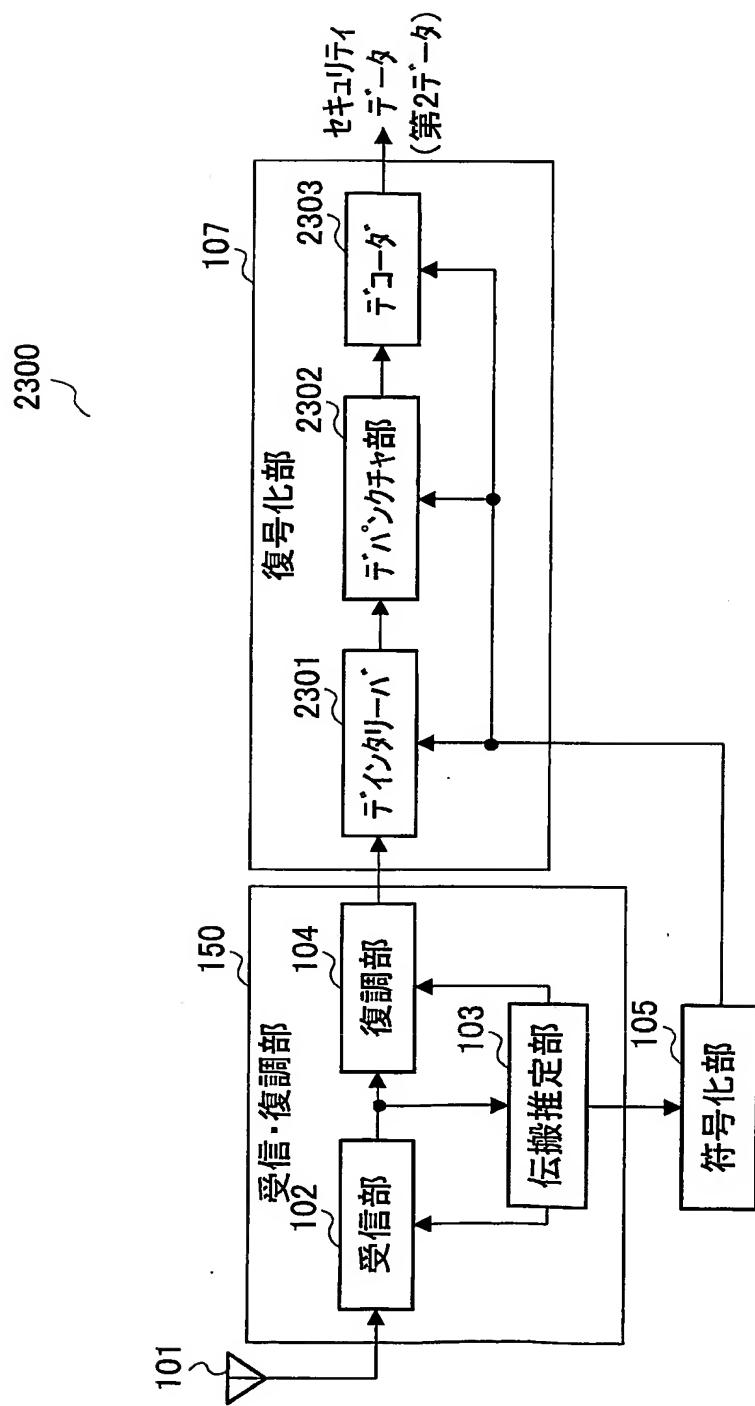


図23

24/78

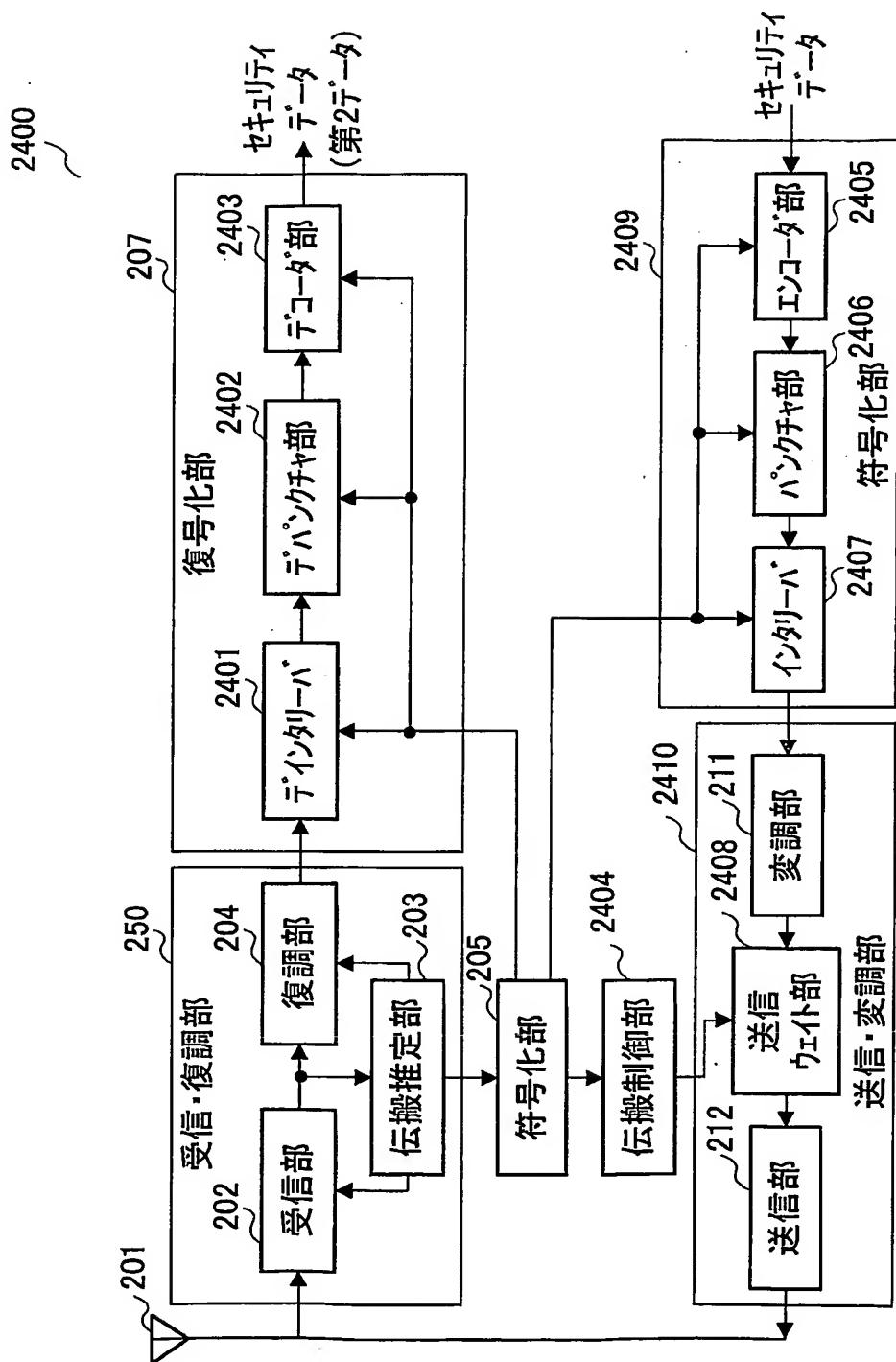


図24

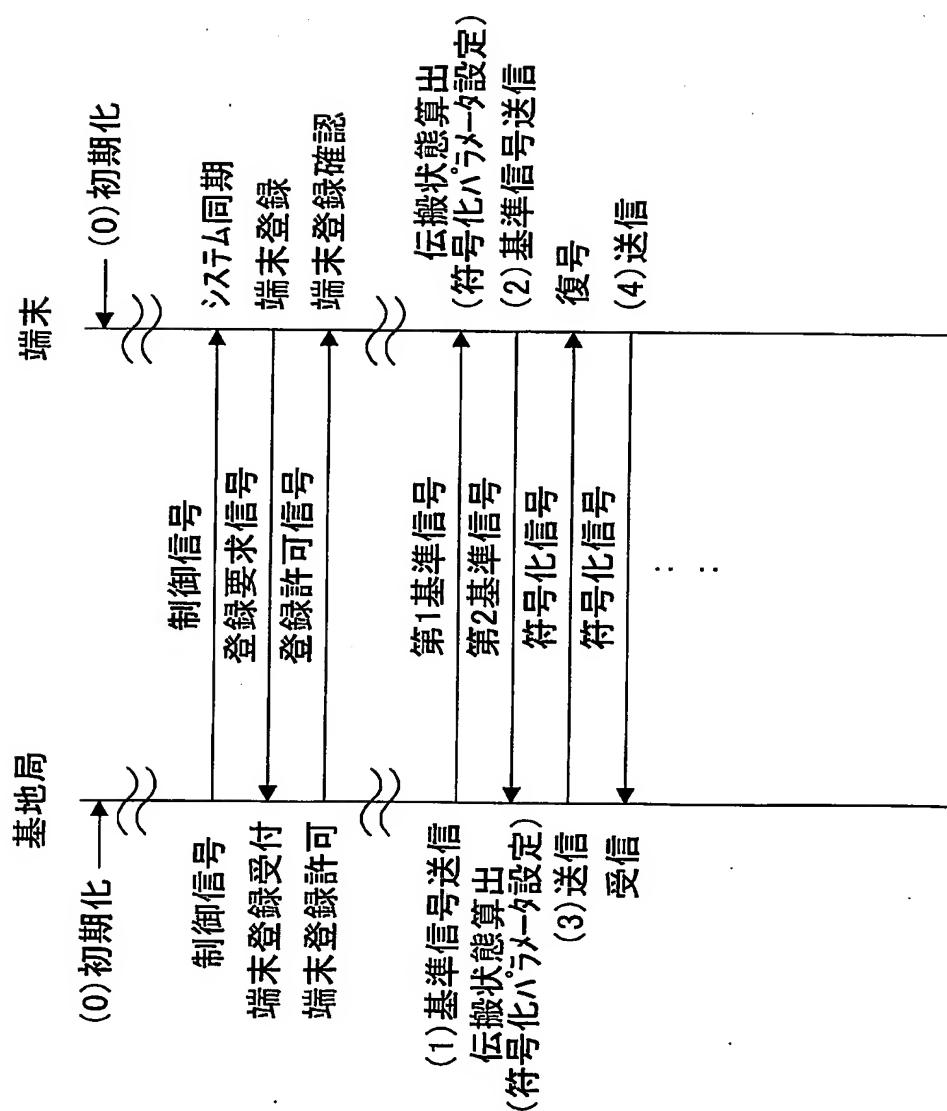


図25

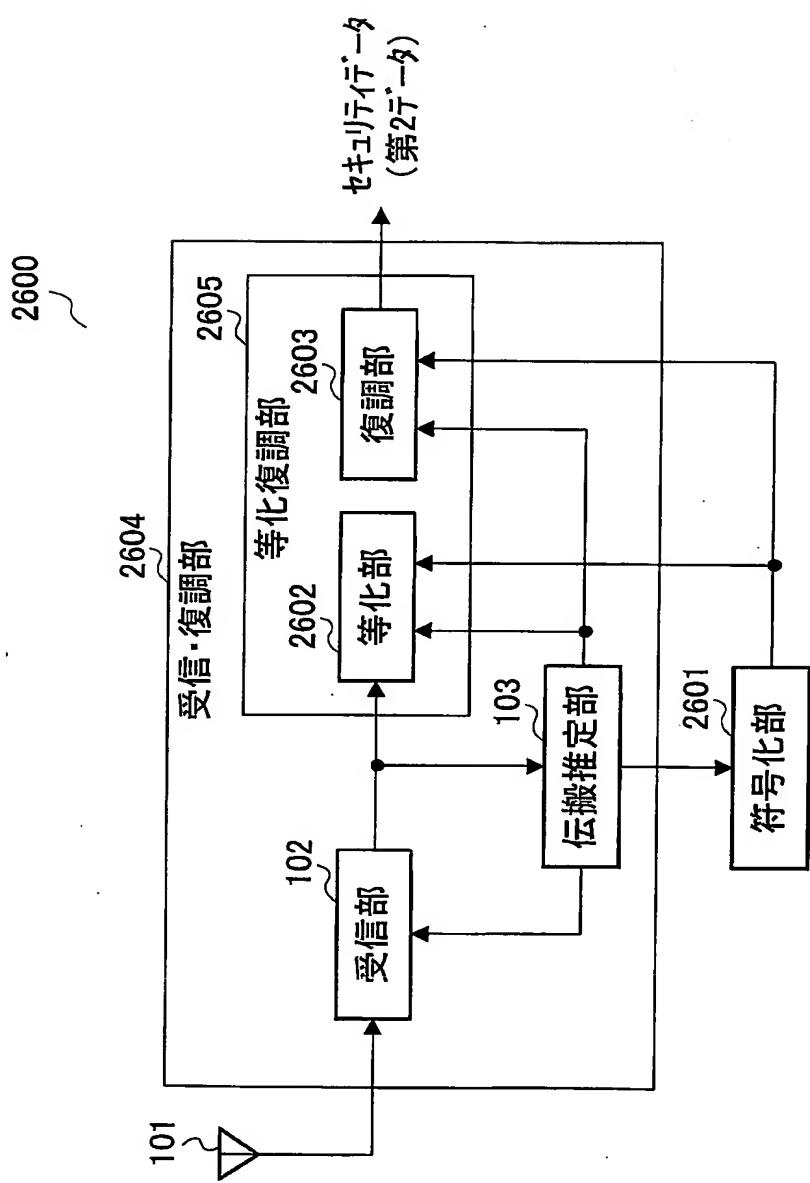


図26

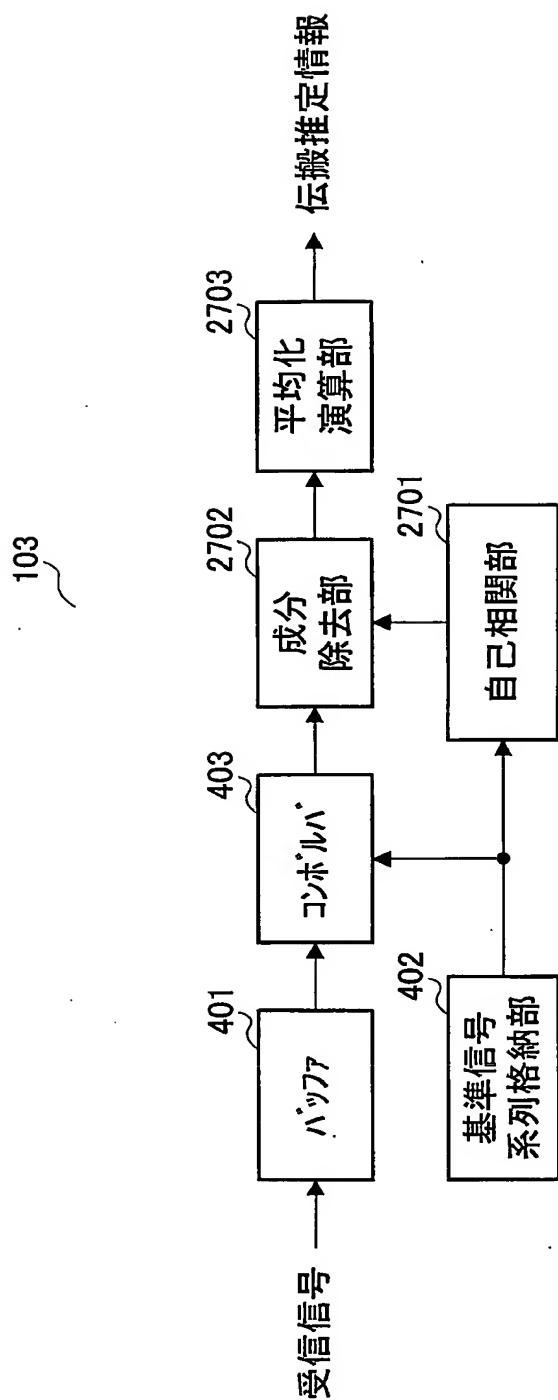


図27

28/78

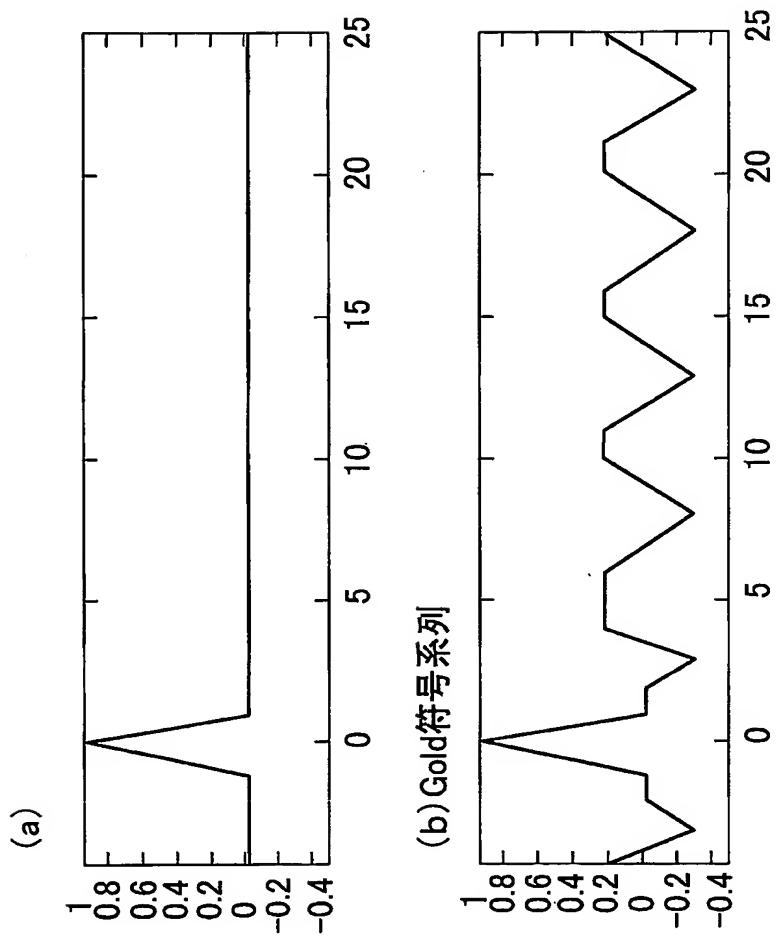


图28

29/78

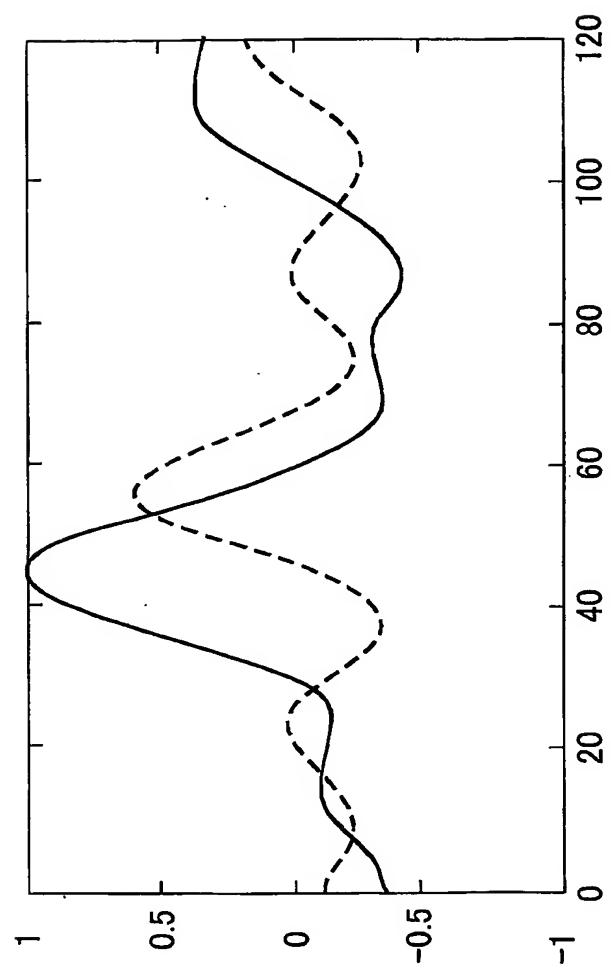


図29

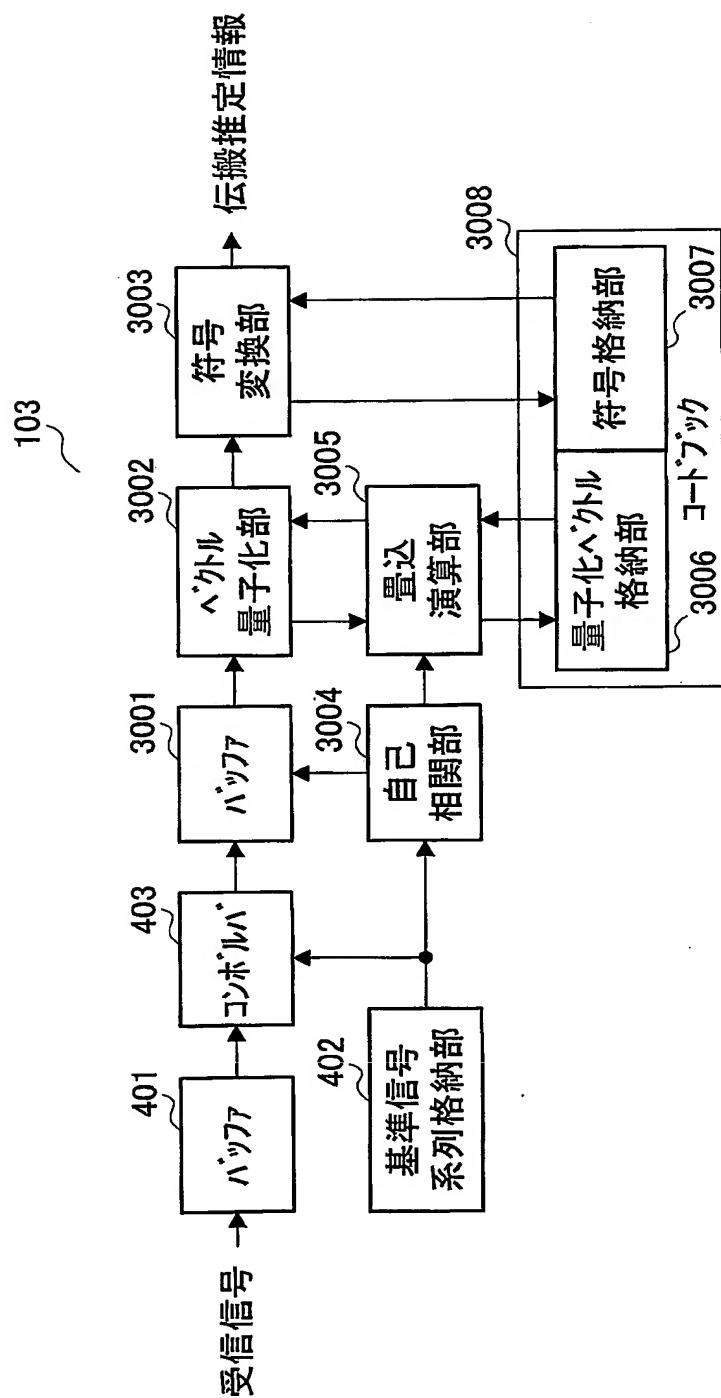


図30

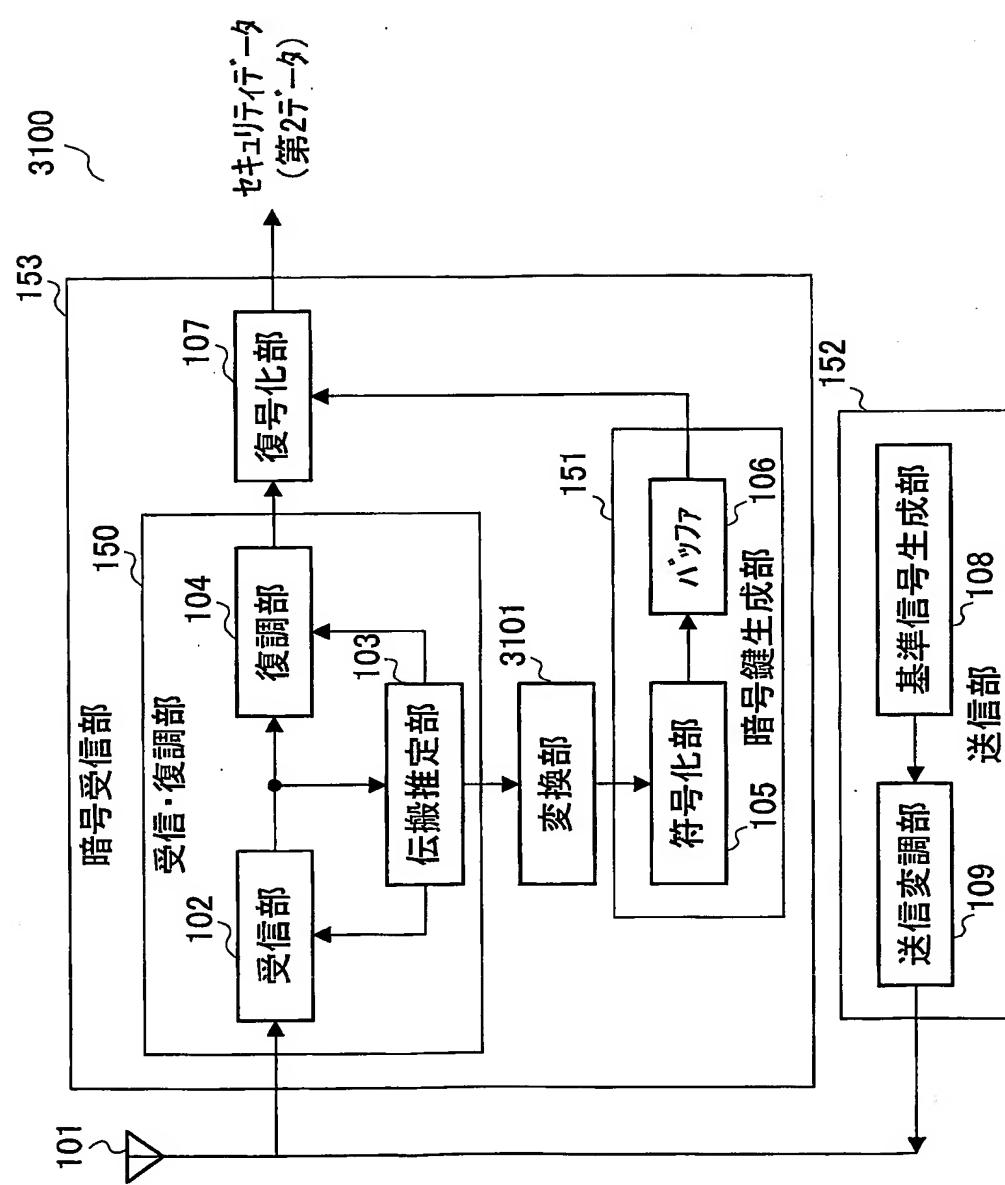


図31

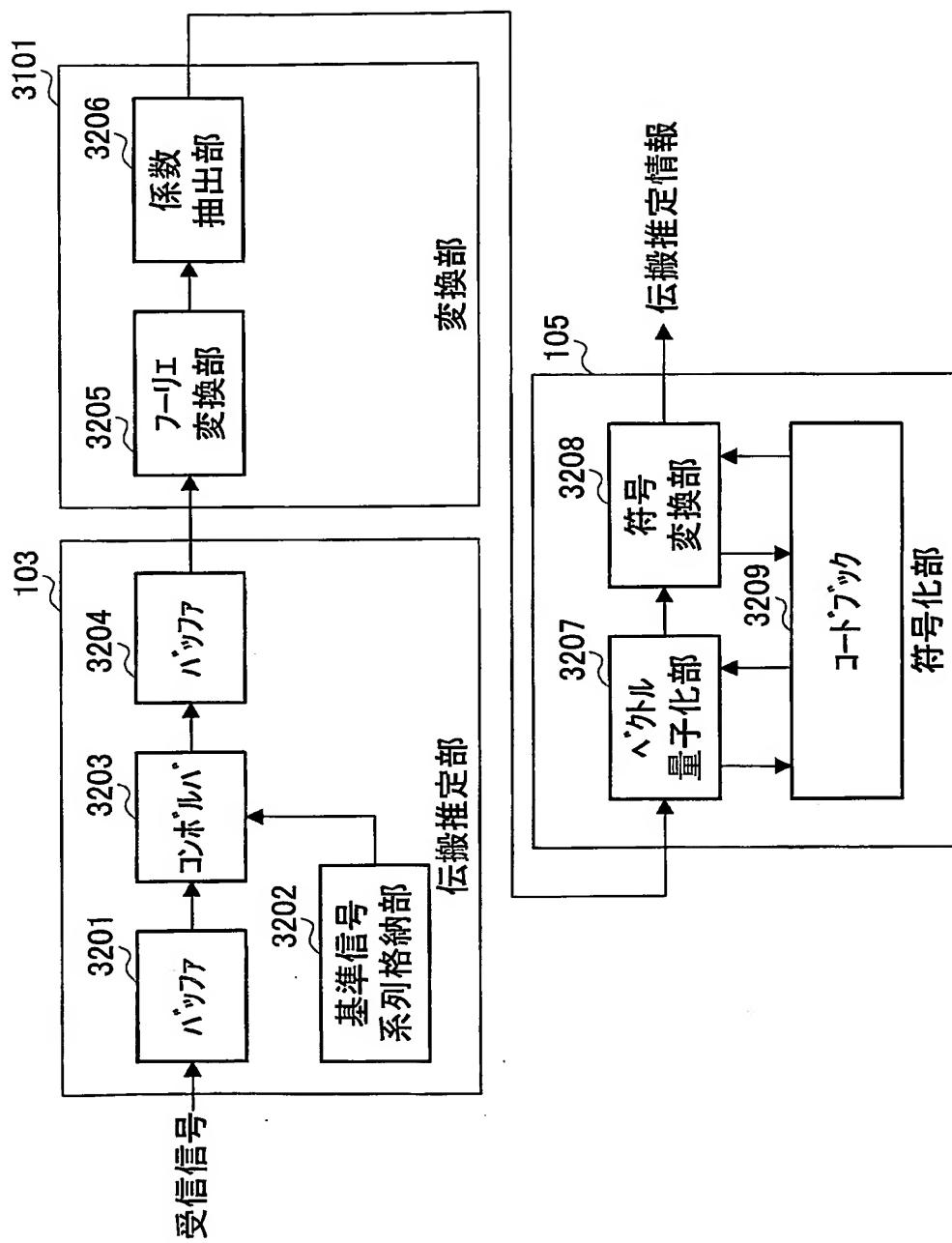


図32

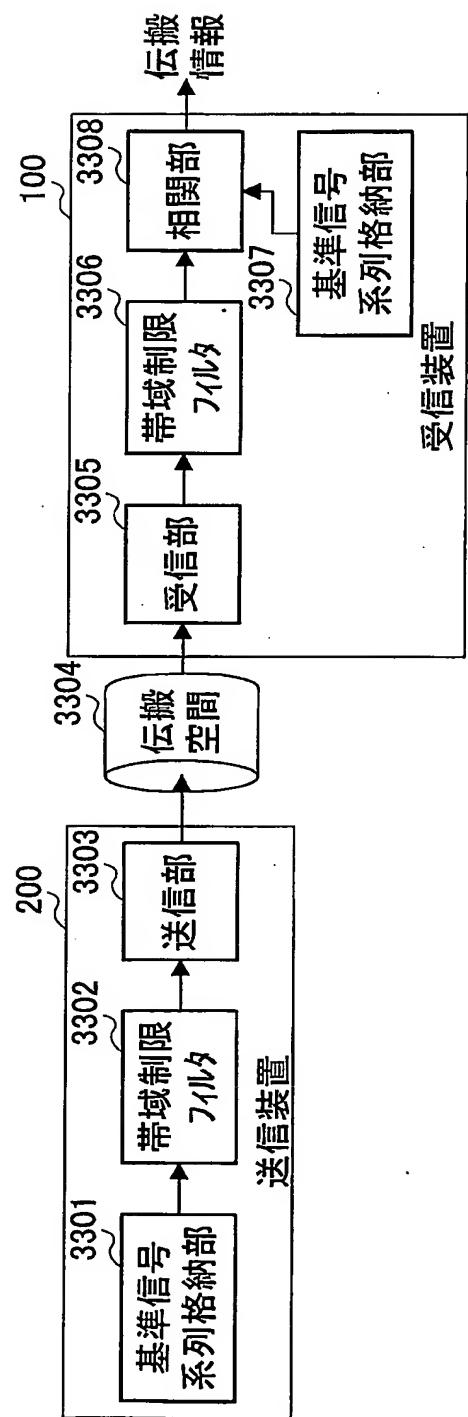


図33

34/78

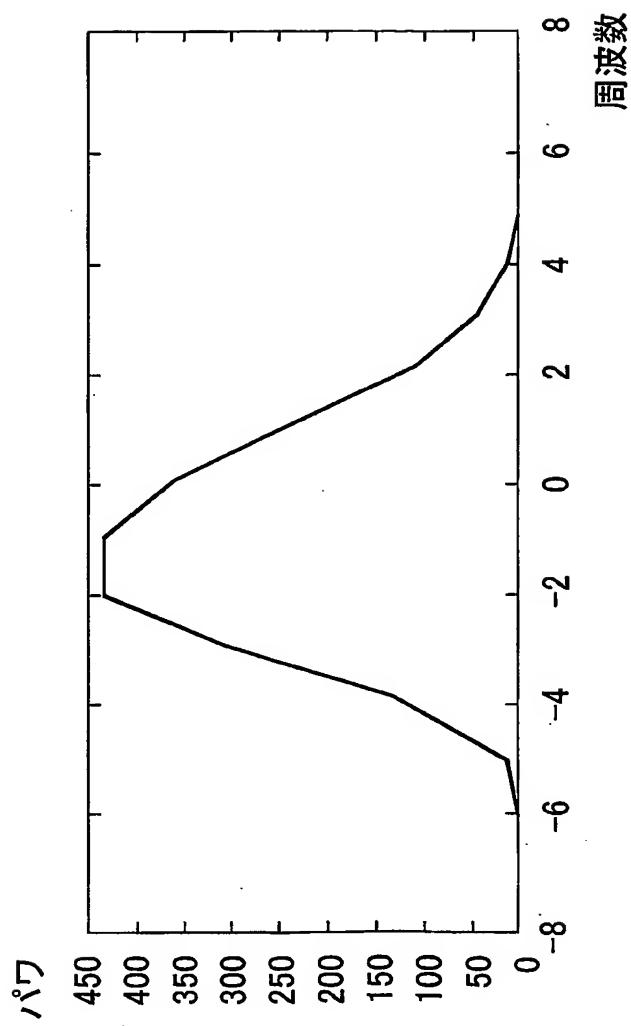


図34

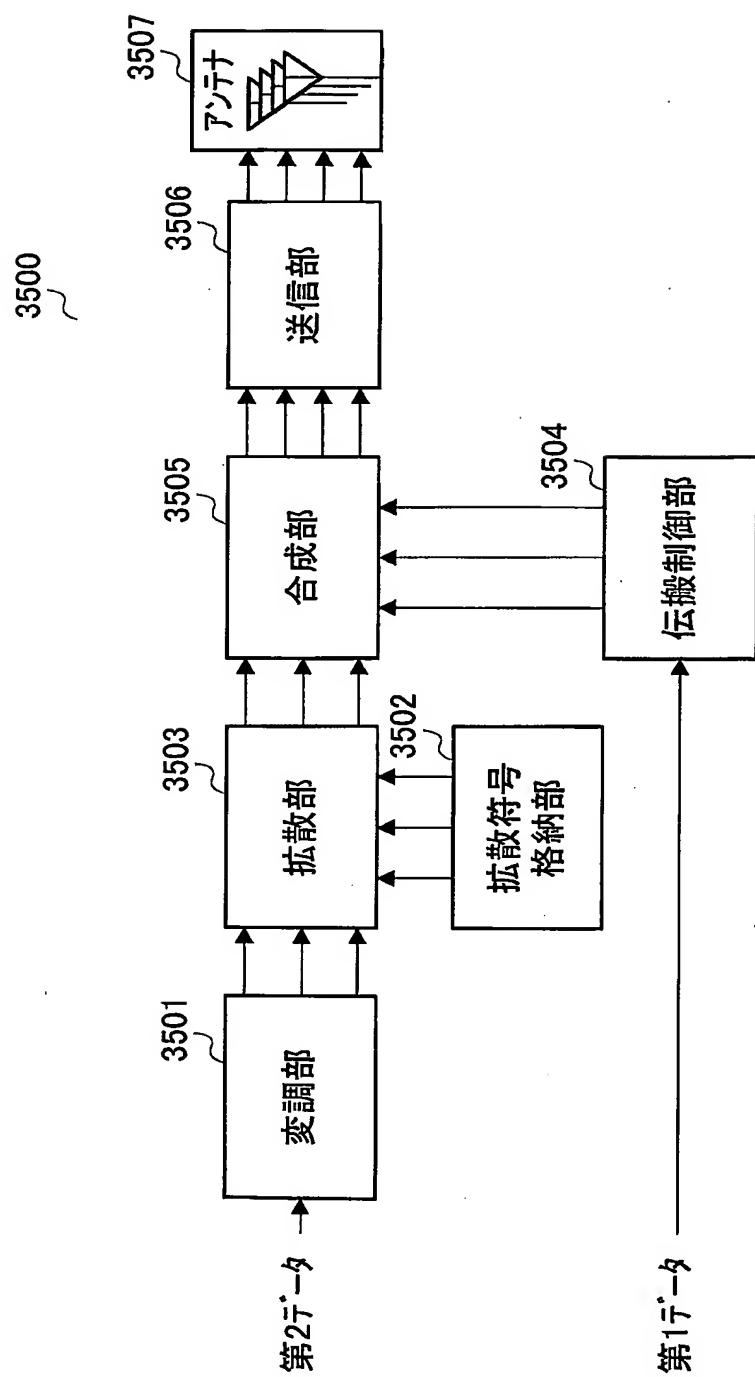


図35

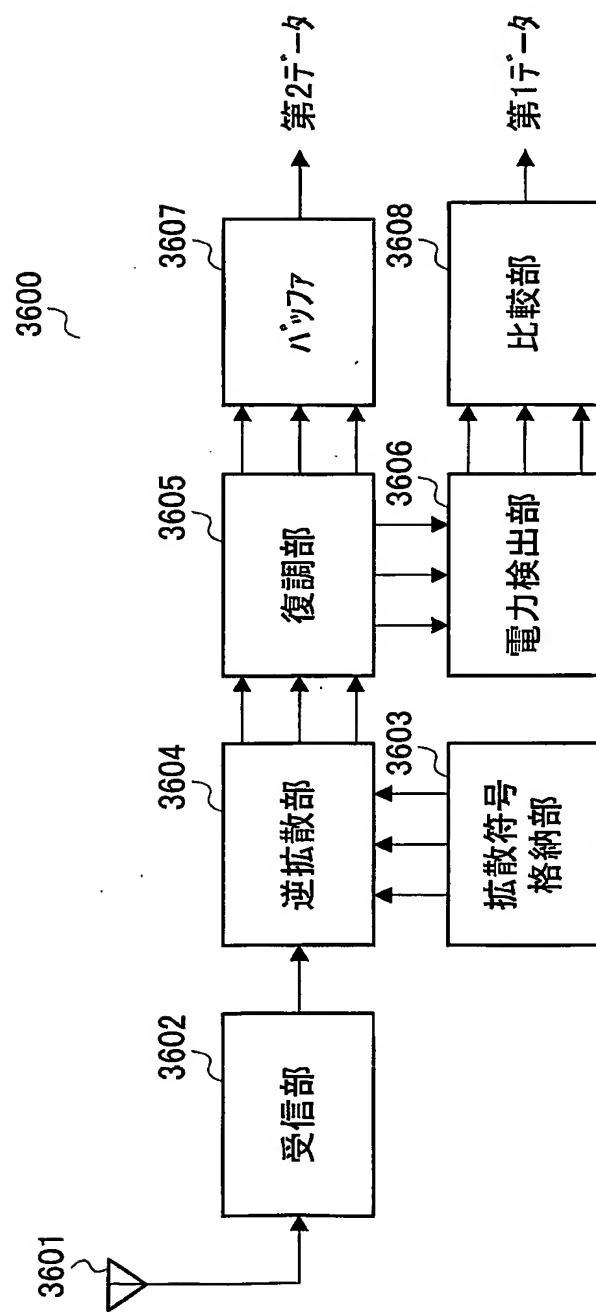


図36

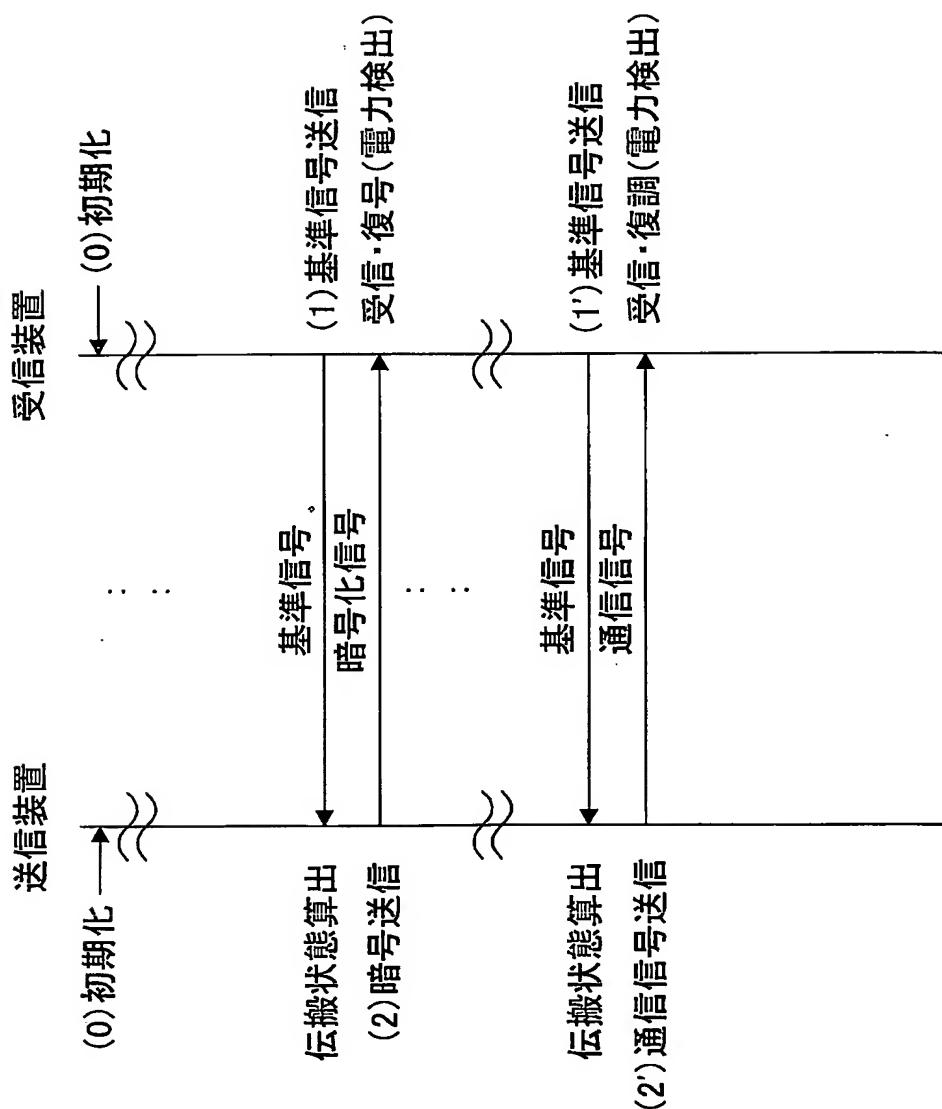


図37

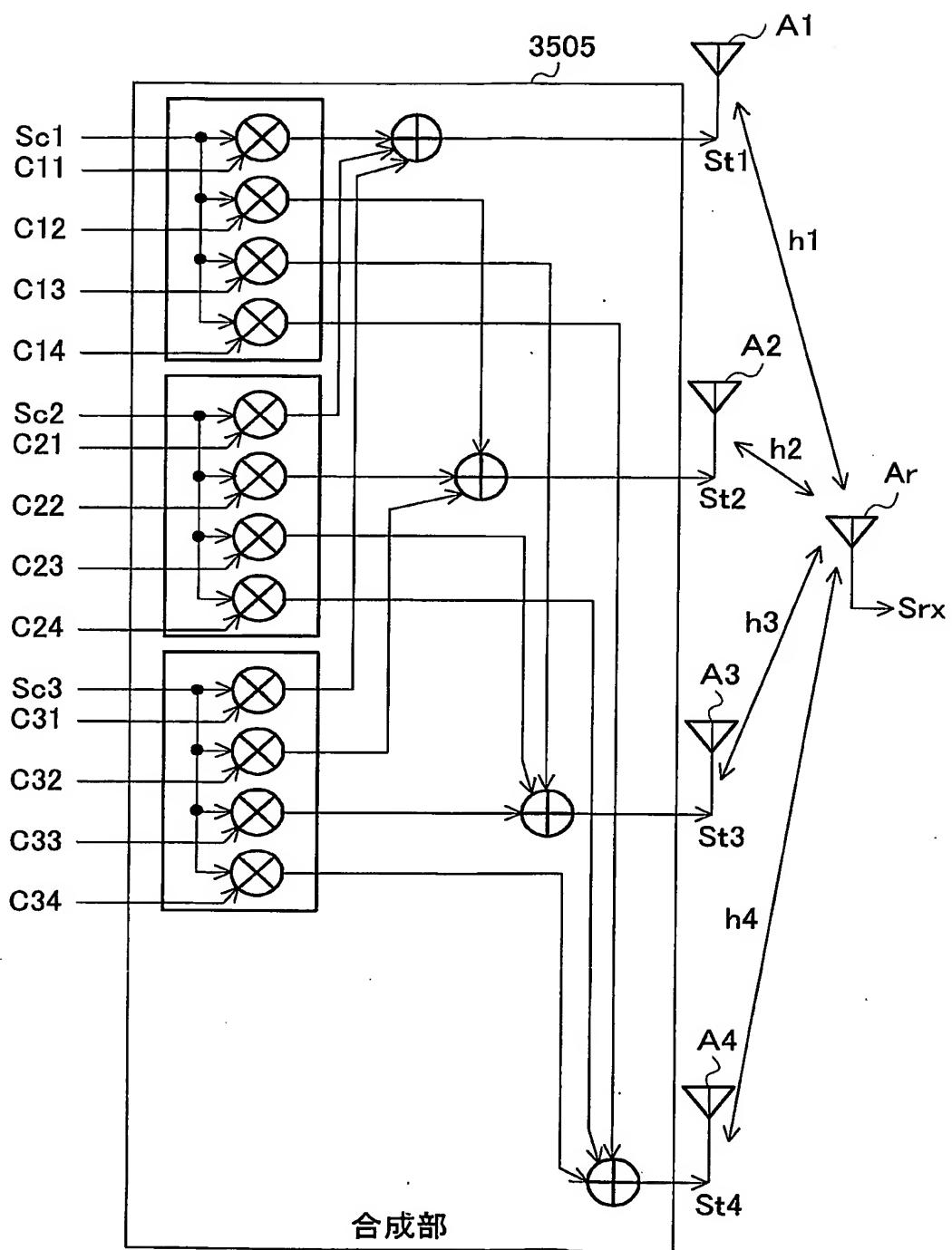


図38

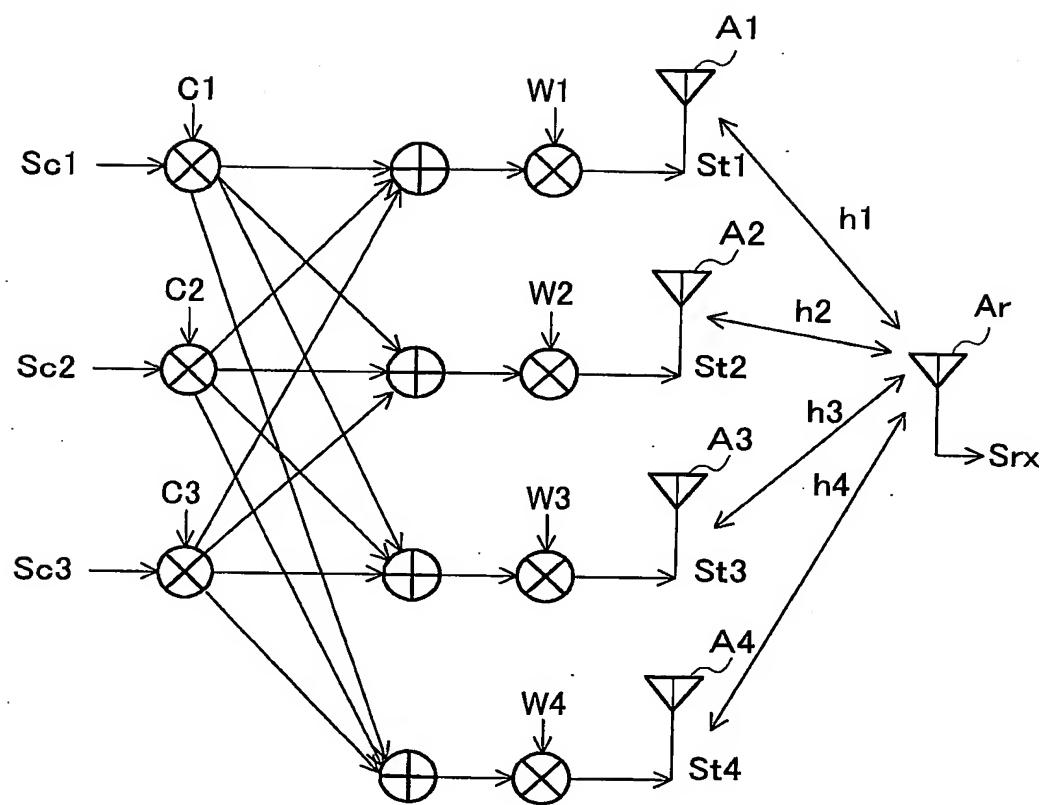


図39

40/78

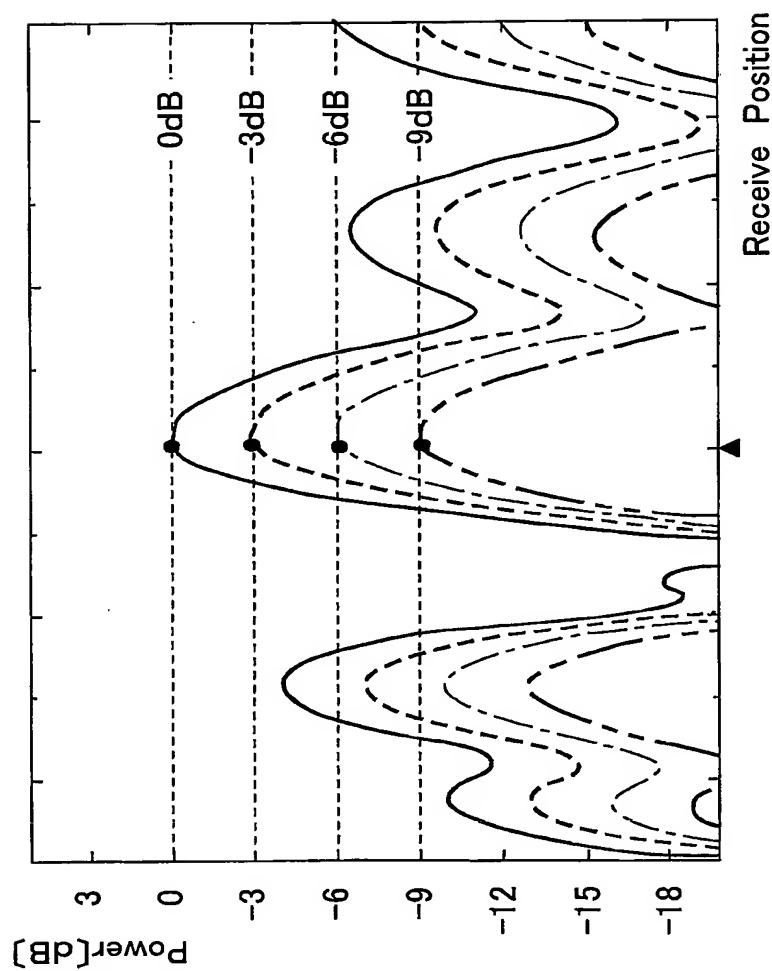


図40

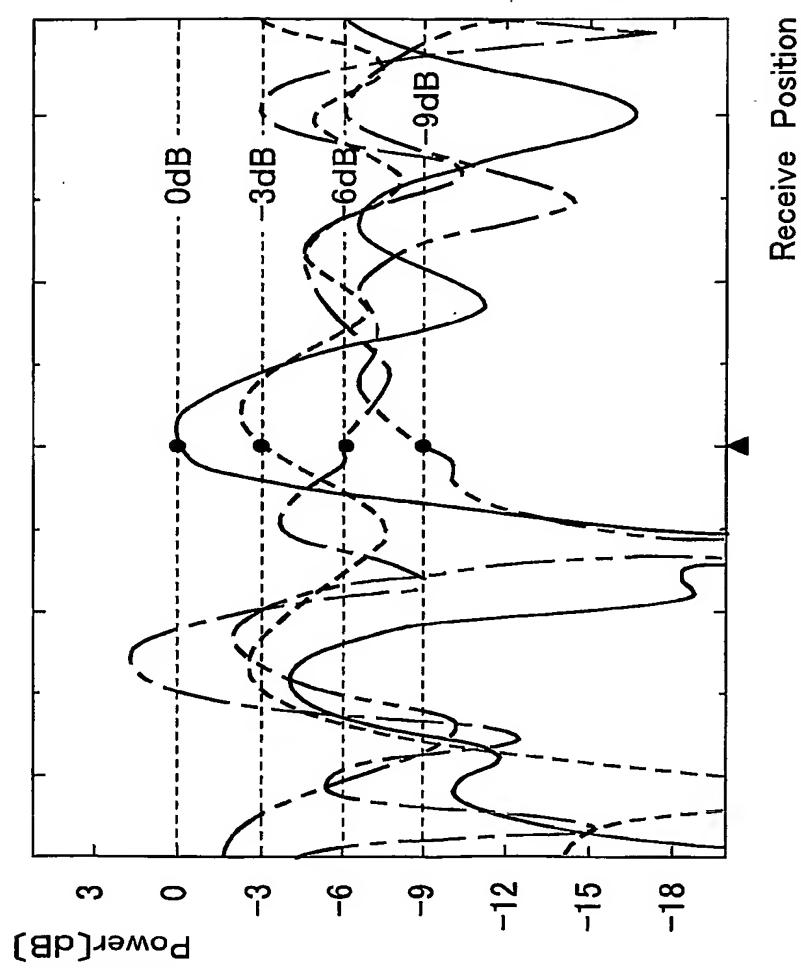


図41

42/78

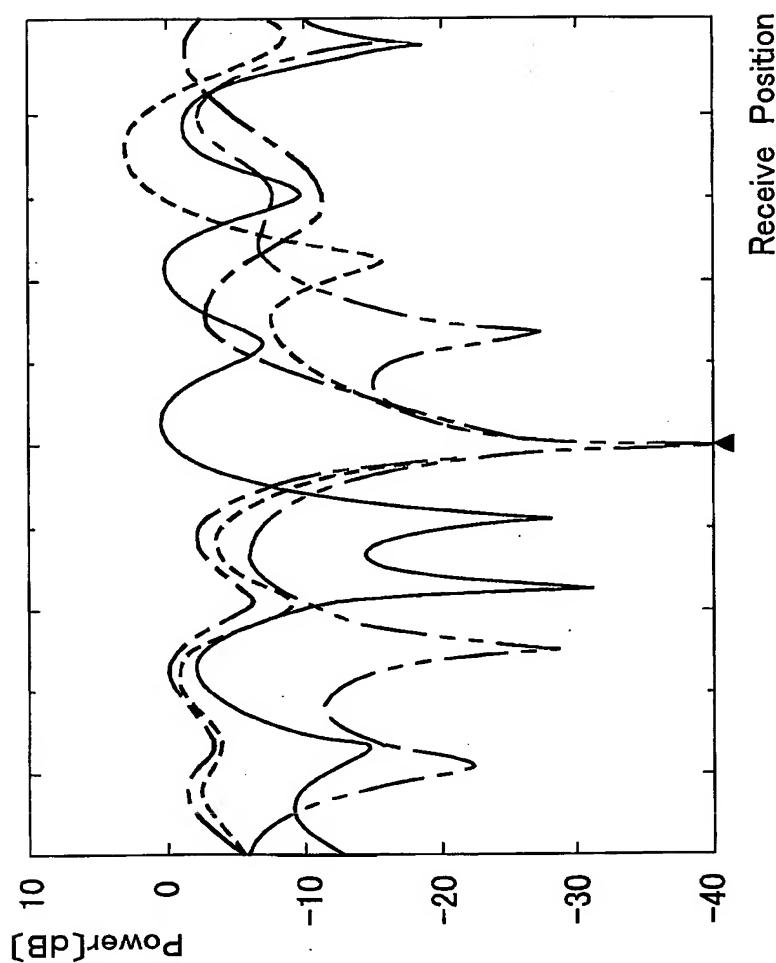


图42

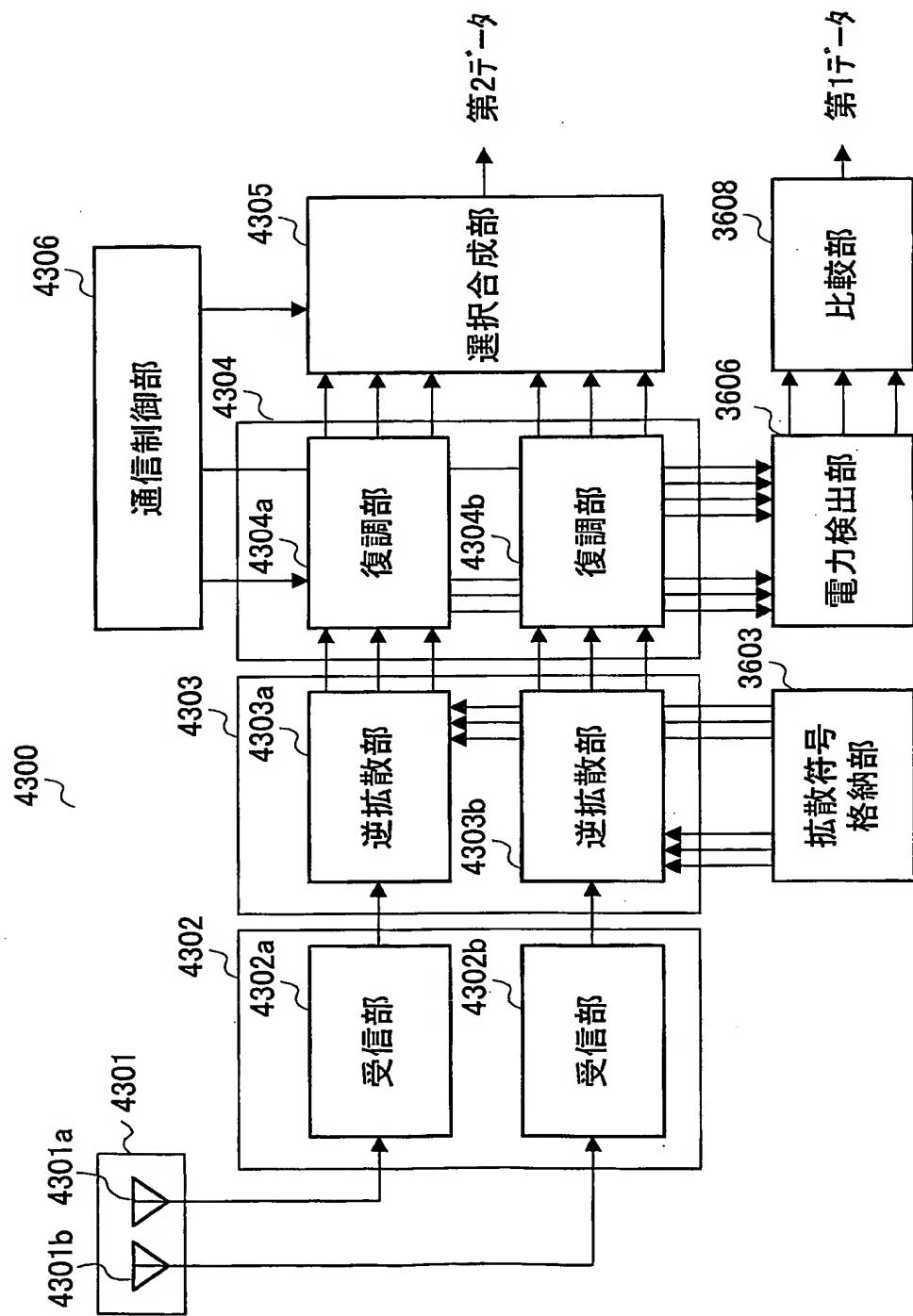


図43

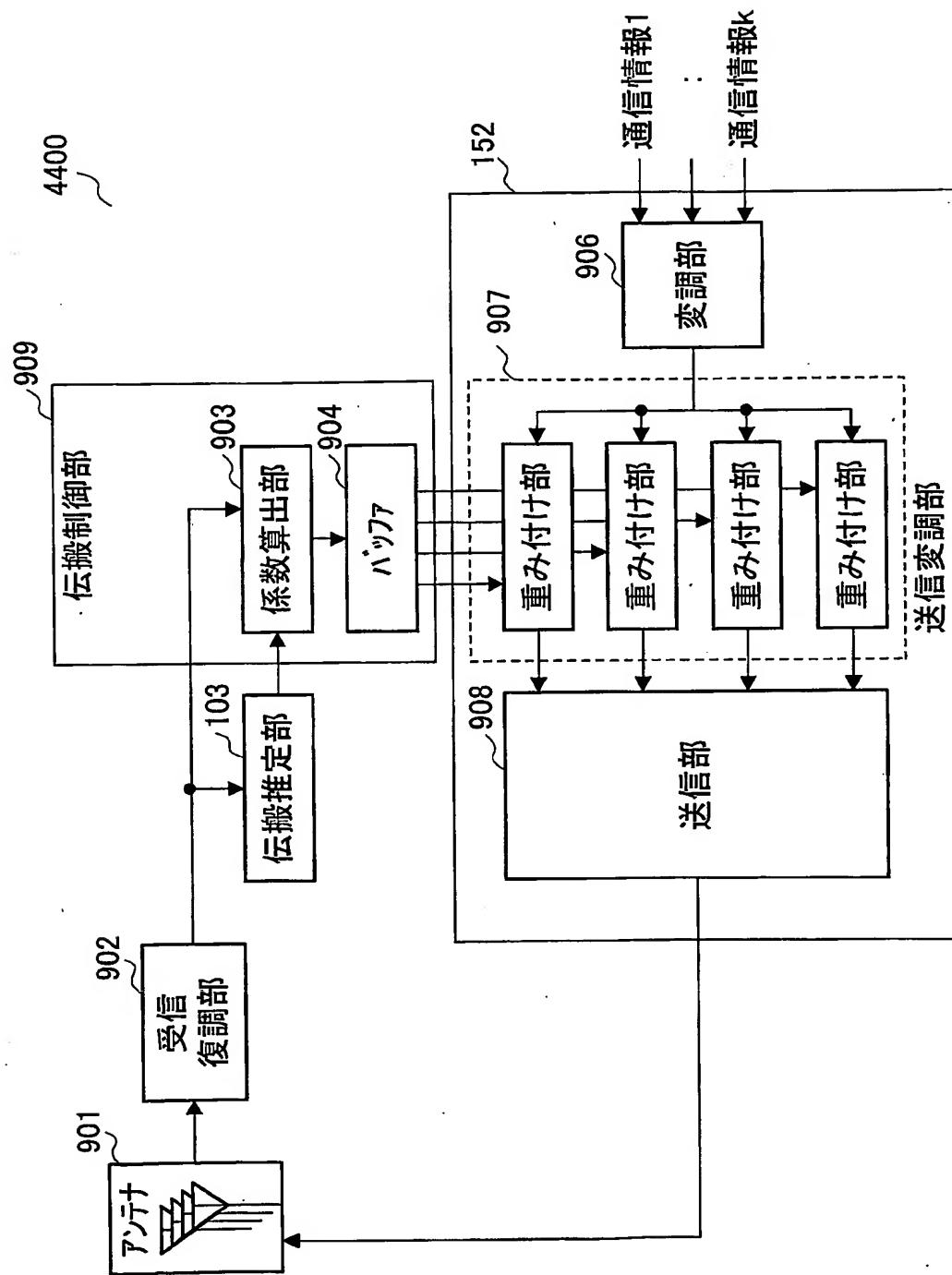


図44

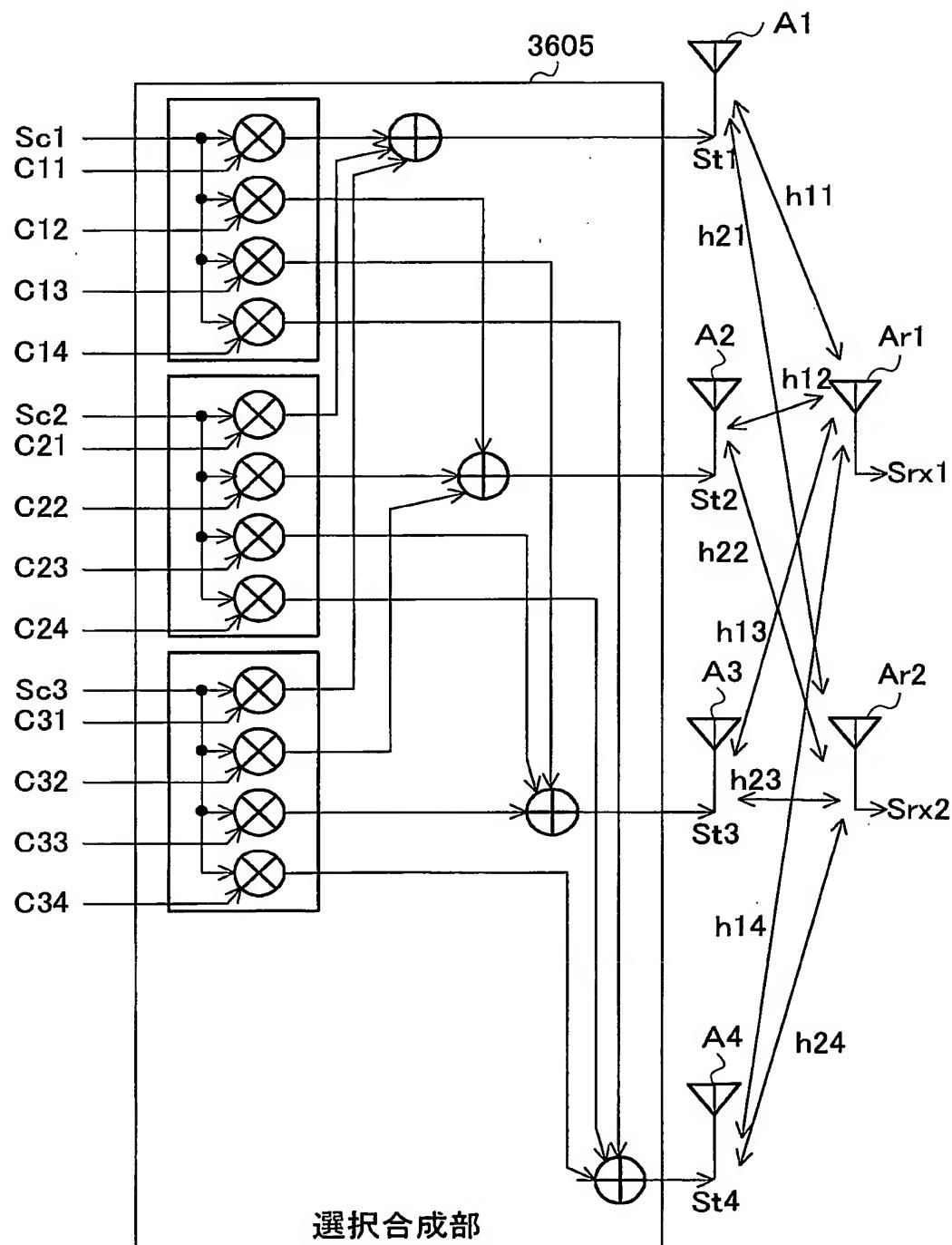


図45

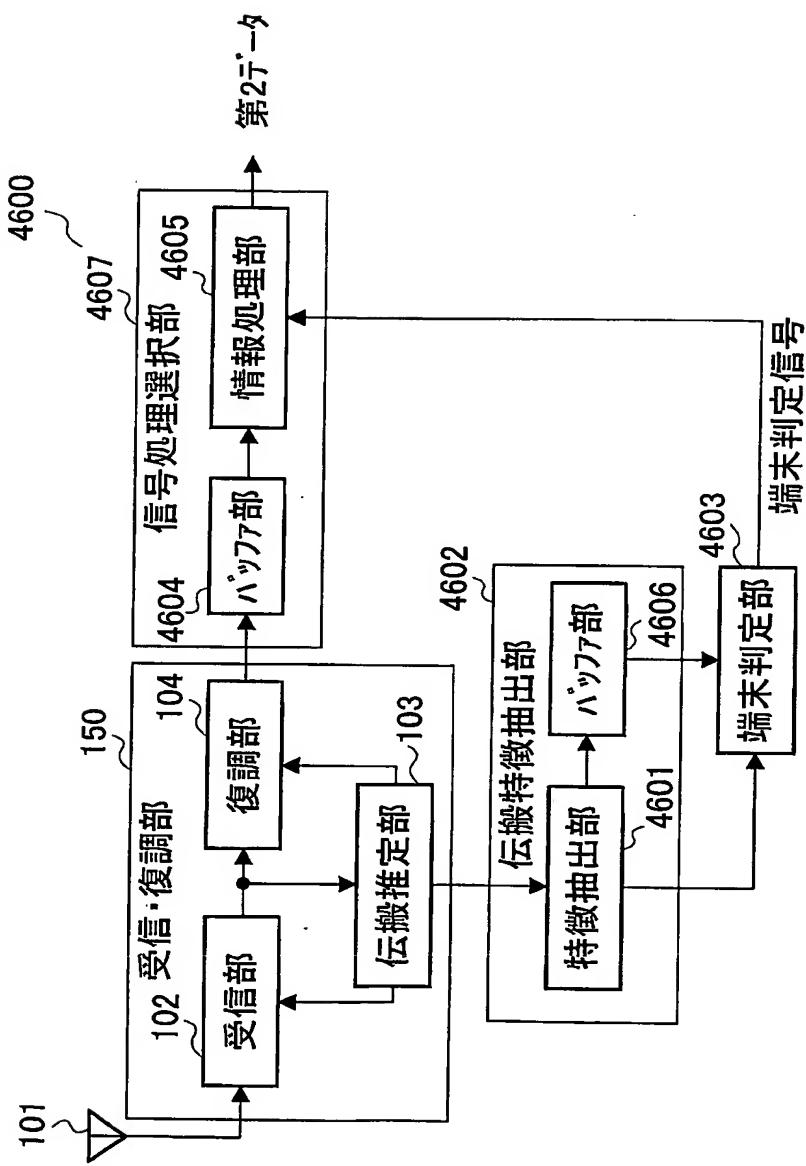


図46

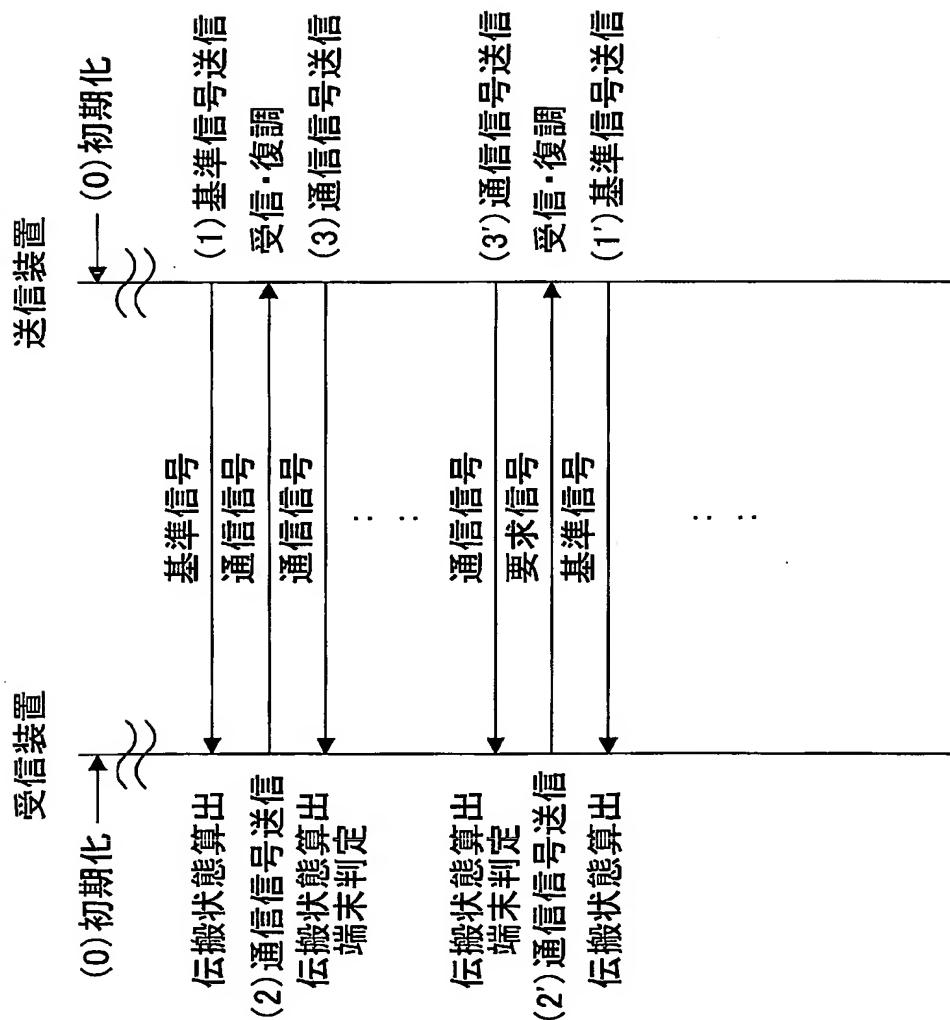


図47

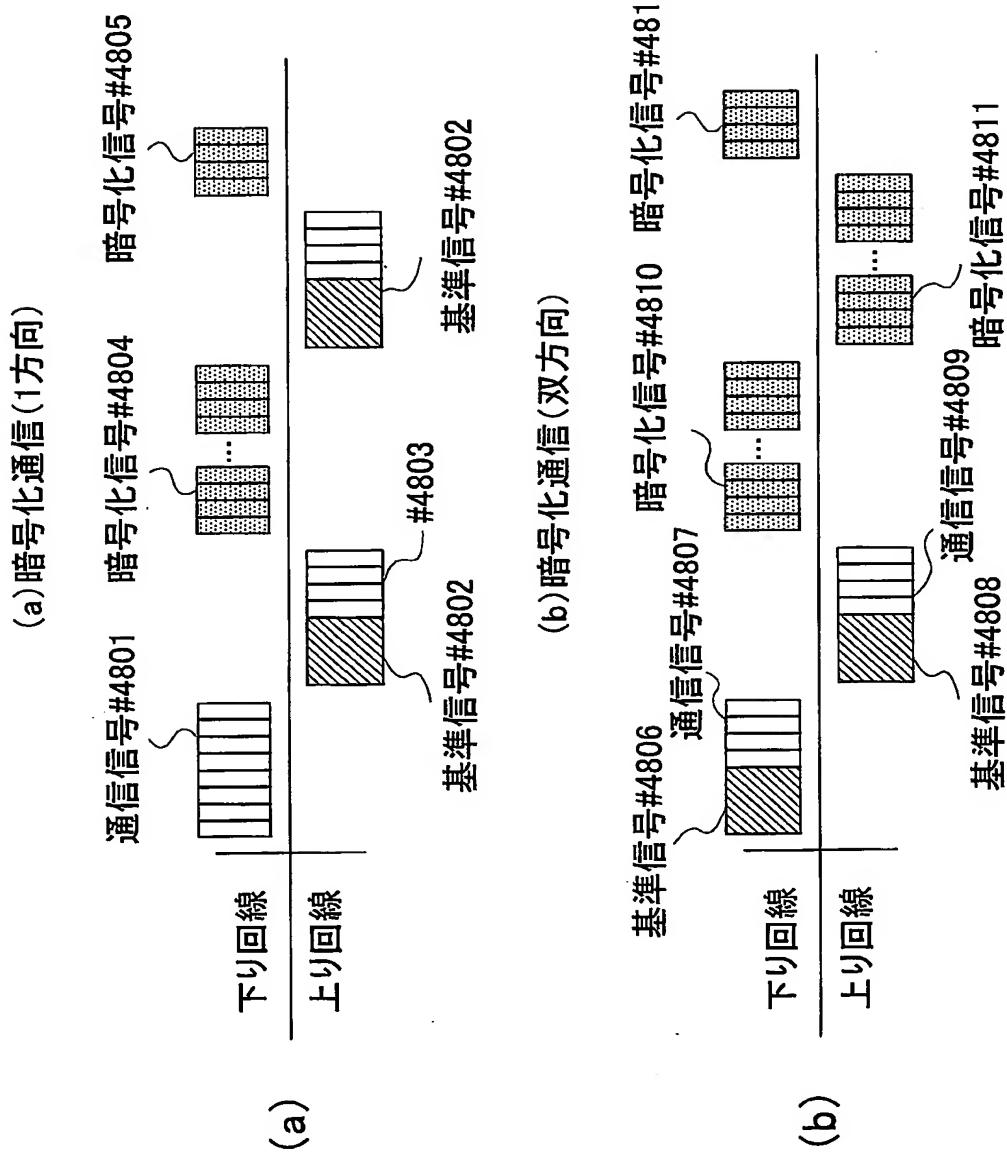


図48

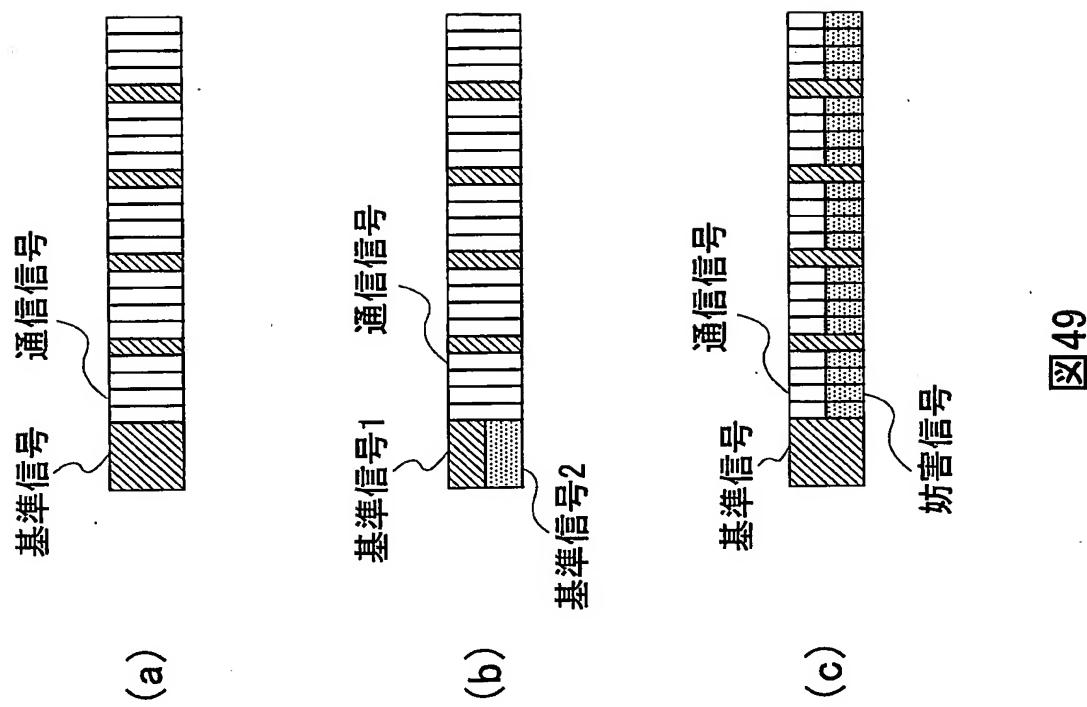


図49

50/78

(a) フレーム構成1

	テ'ークn	テ'ークn	テ'ークn	テ'ークn	テ'ークn
:	:	:	:	:	:
バイロット信号	テ'ーク2	テ'ーク2	テ'ーク2	テ'ーク2	テ'ーク2
	テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1

(b) フレーム構成2

	テ'ークn	テ'ークn	テ'ークn	テ'ークn	テ'ークn
:	:	:	:	:	:
テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1
バイロット信号	バイロット信号	バイロット信号	バイロット信号	バイロット信号	バイロット信号

(c) フレーム構成3

	テ'ークn	テ'ークn	テ'ークn	テ'ークn	テ'ークn
:	:	:	:	:	:
バイロット信号n	バイロット信号n	バイロット信号n	バイロット信号n	バイロット信号n	バイロット信号n
	テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1	テ'ーク1
バイロット信号1	バイロット信号1	バイロット信号1	バイロット信号1	バイロット信号1	バイロット信号1

図50

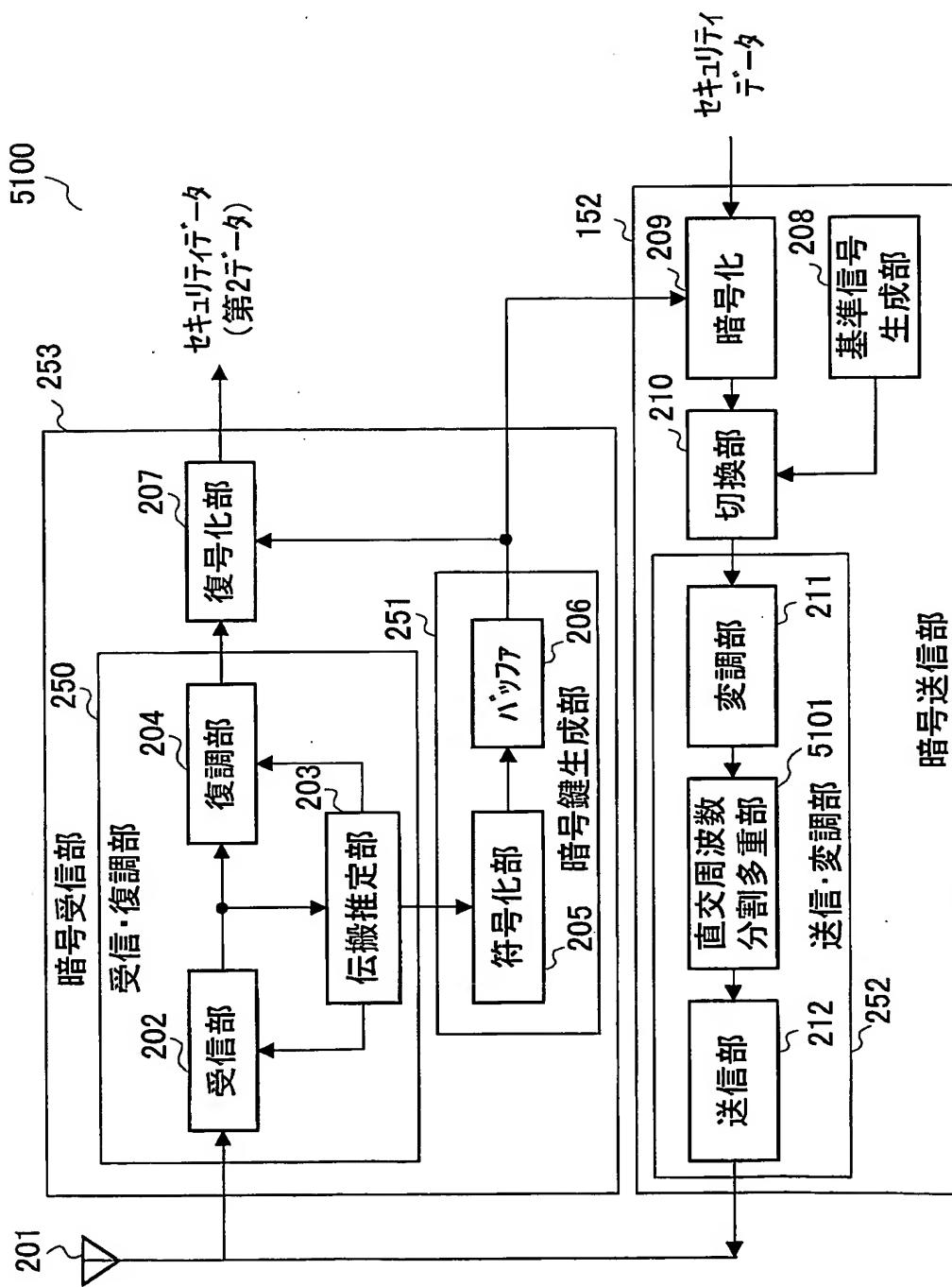


図51

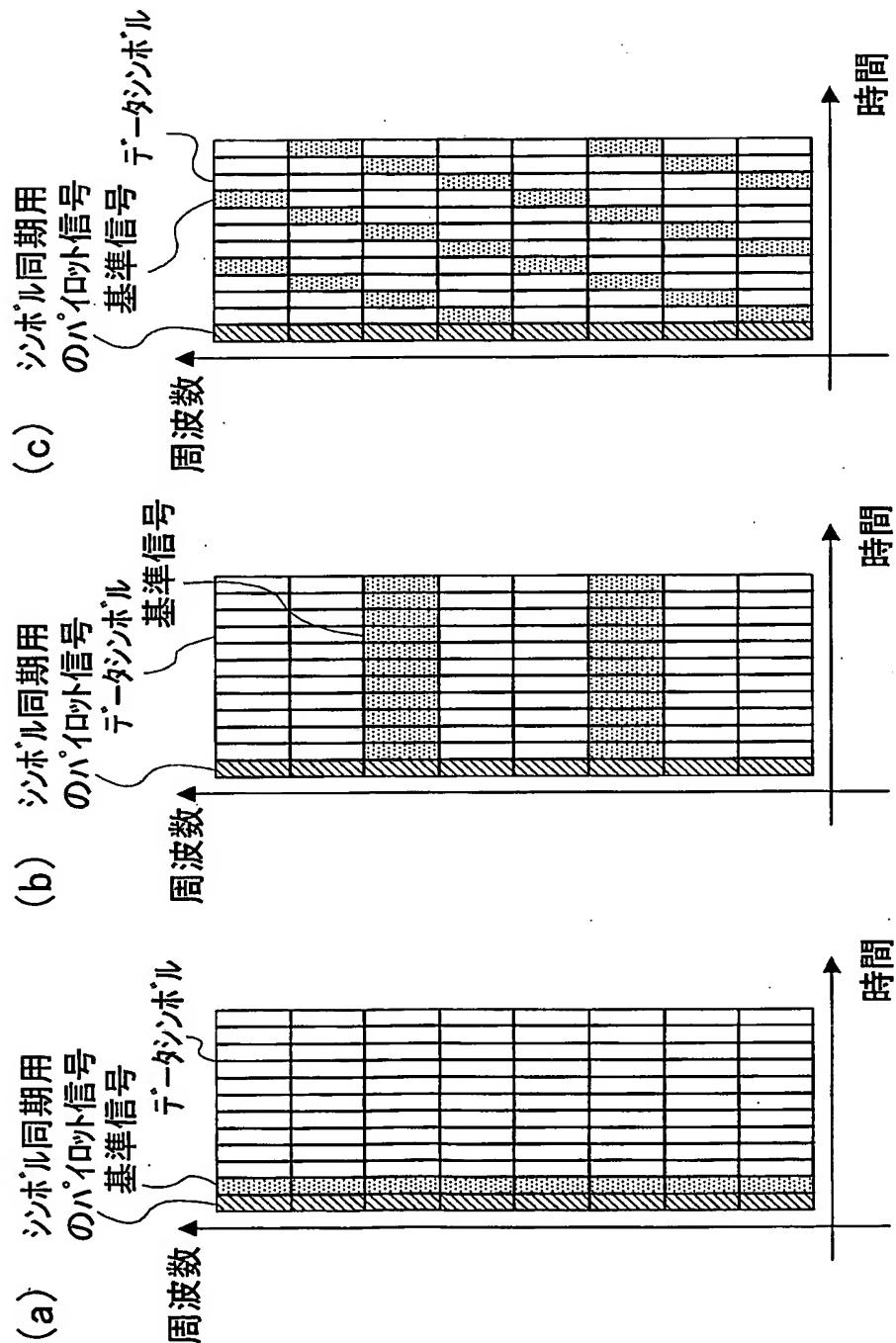
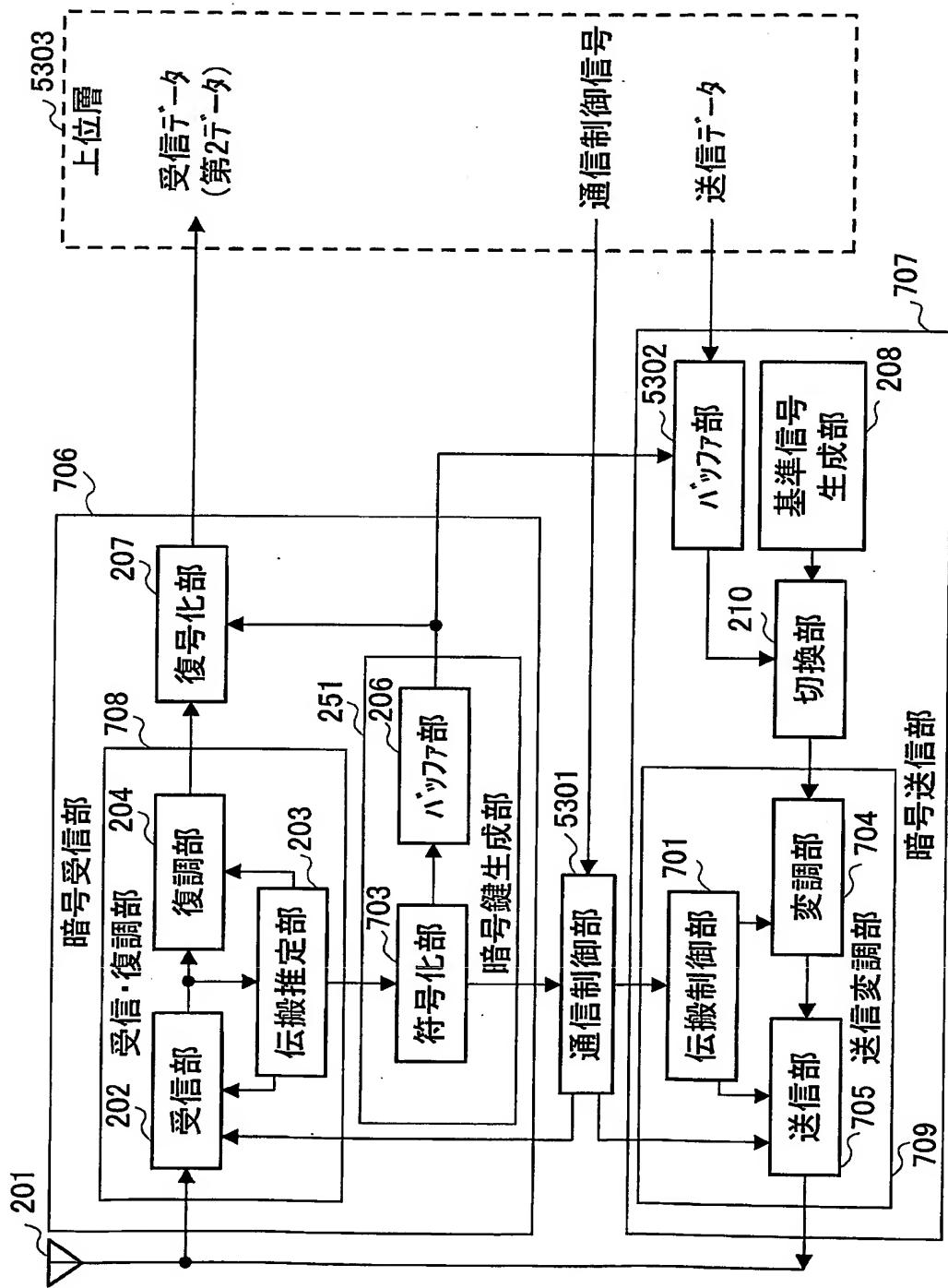


図52



53

54/78

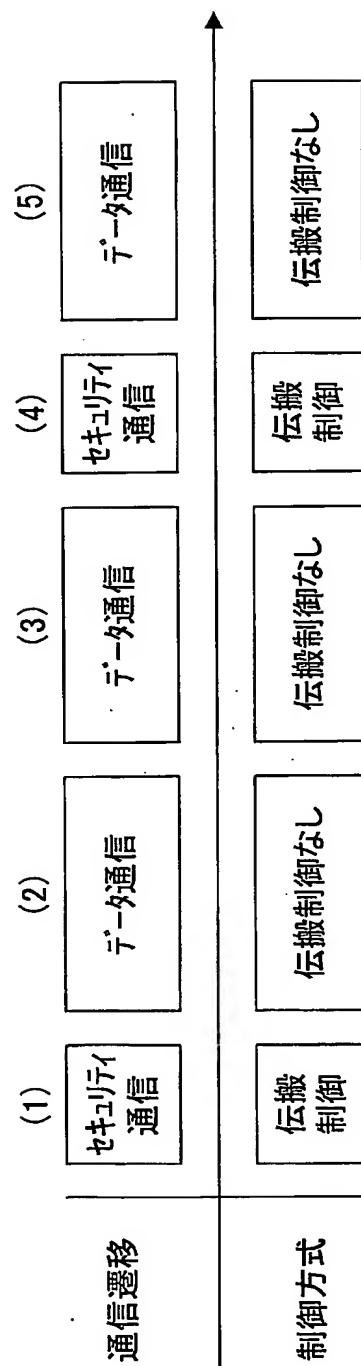


図54

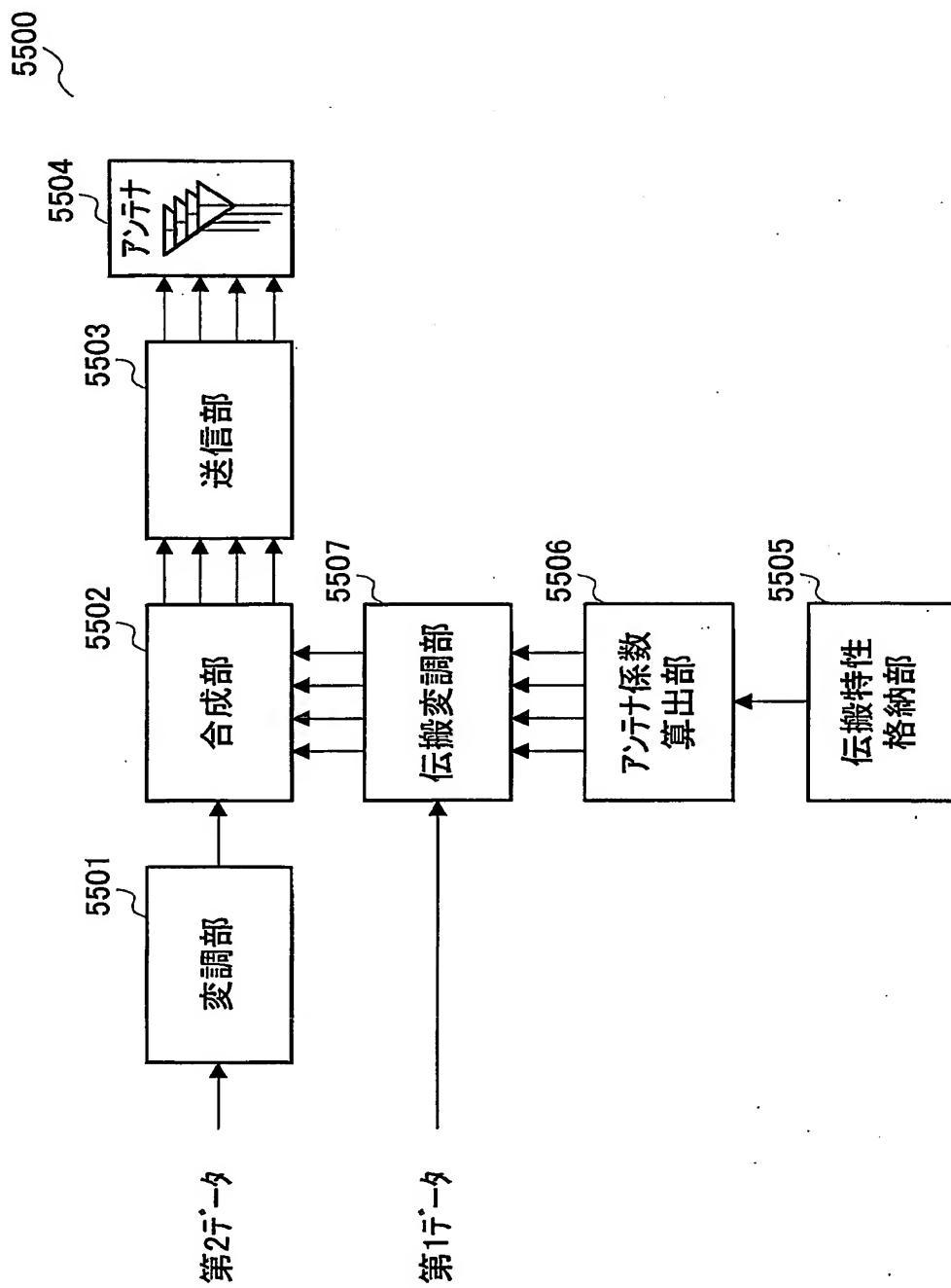


図55

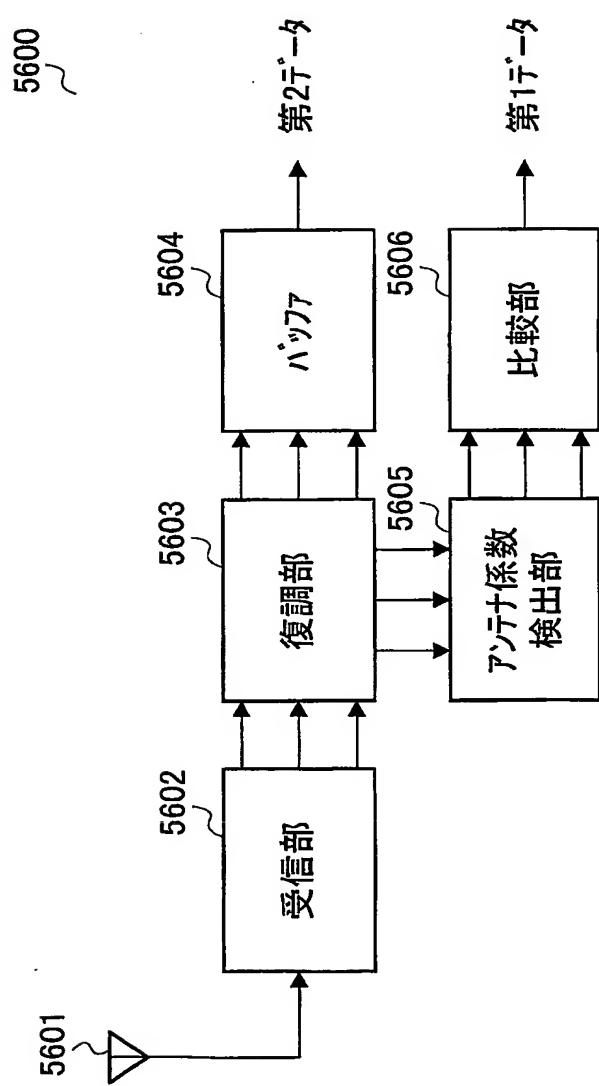


図56

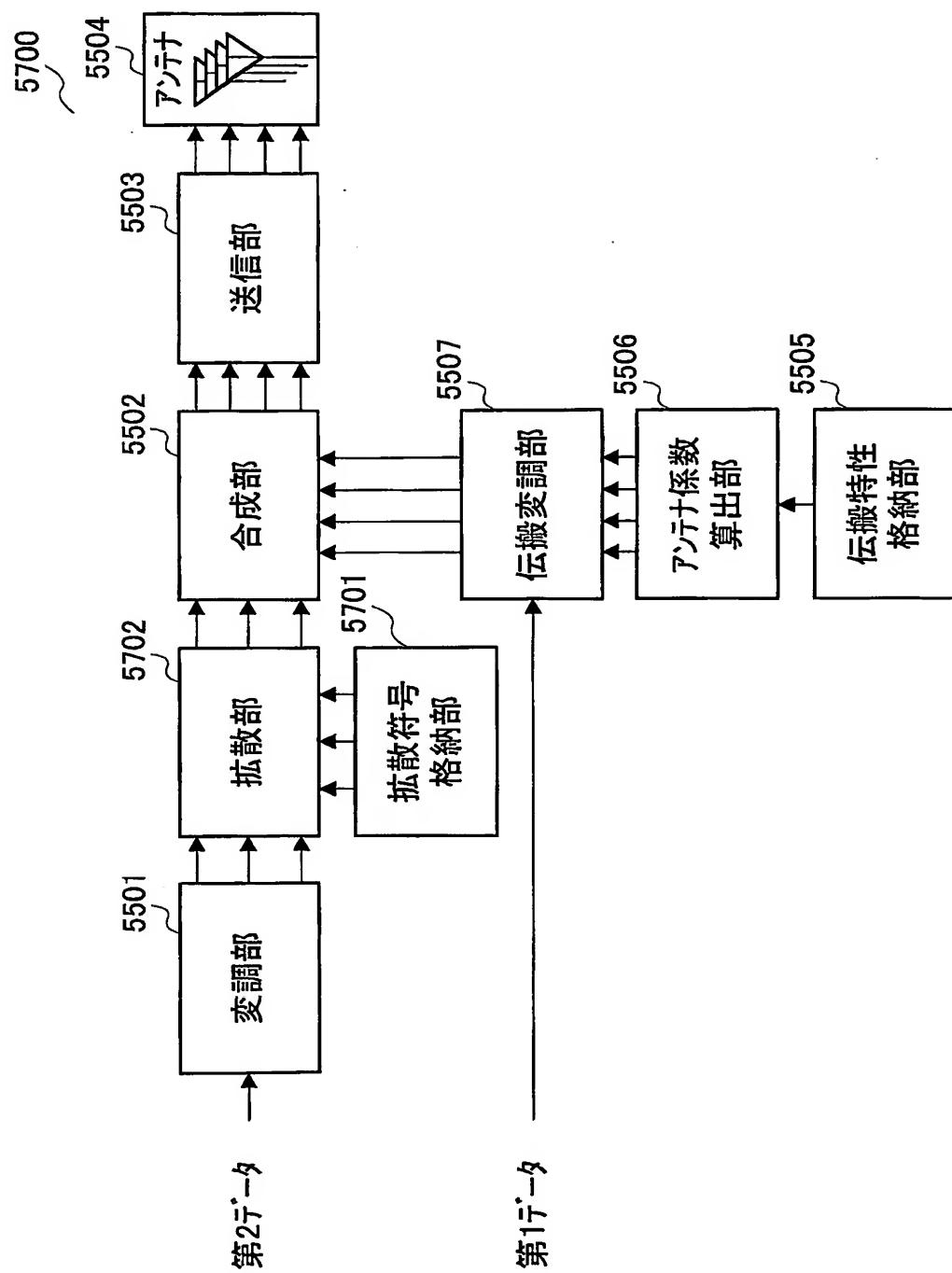


図57

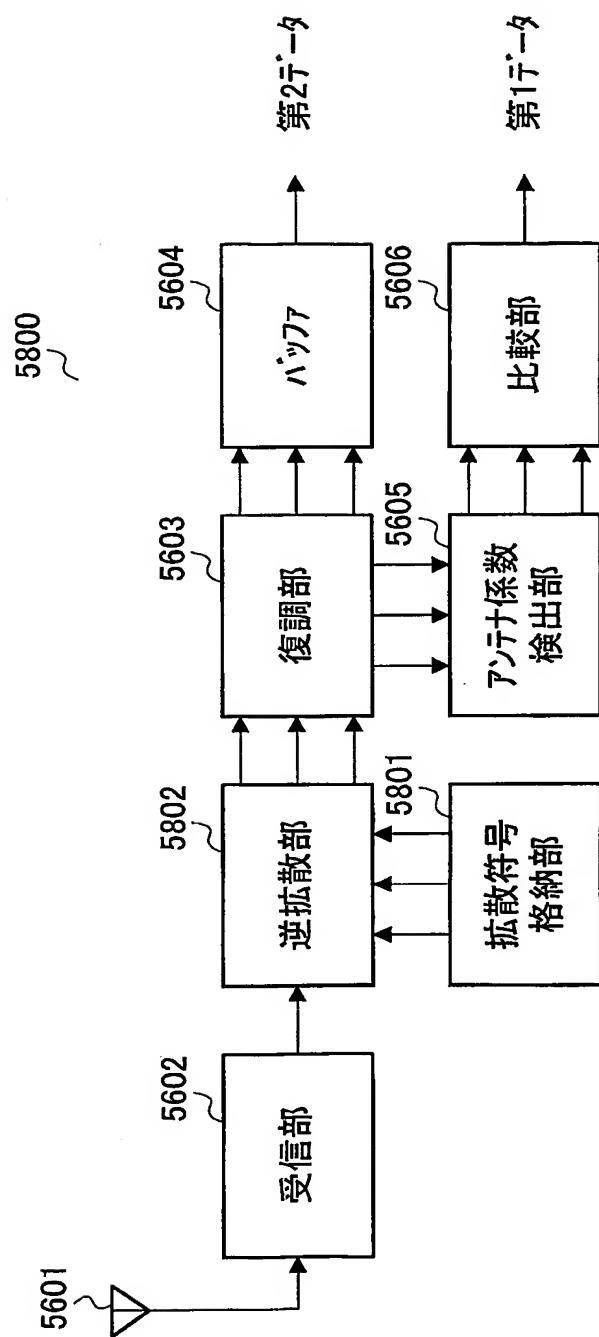


図58

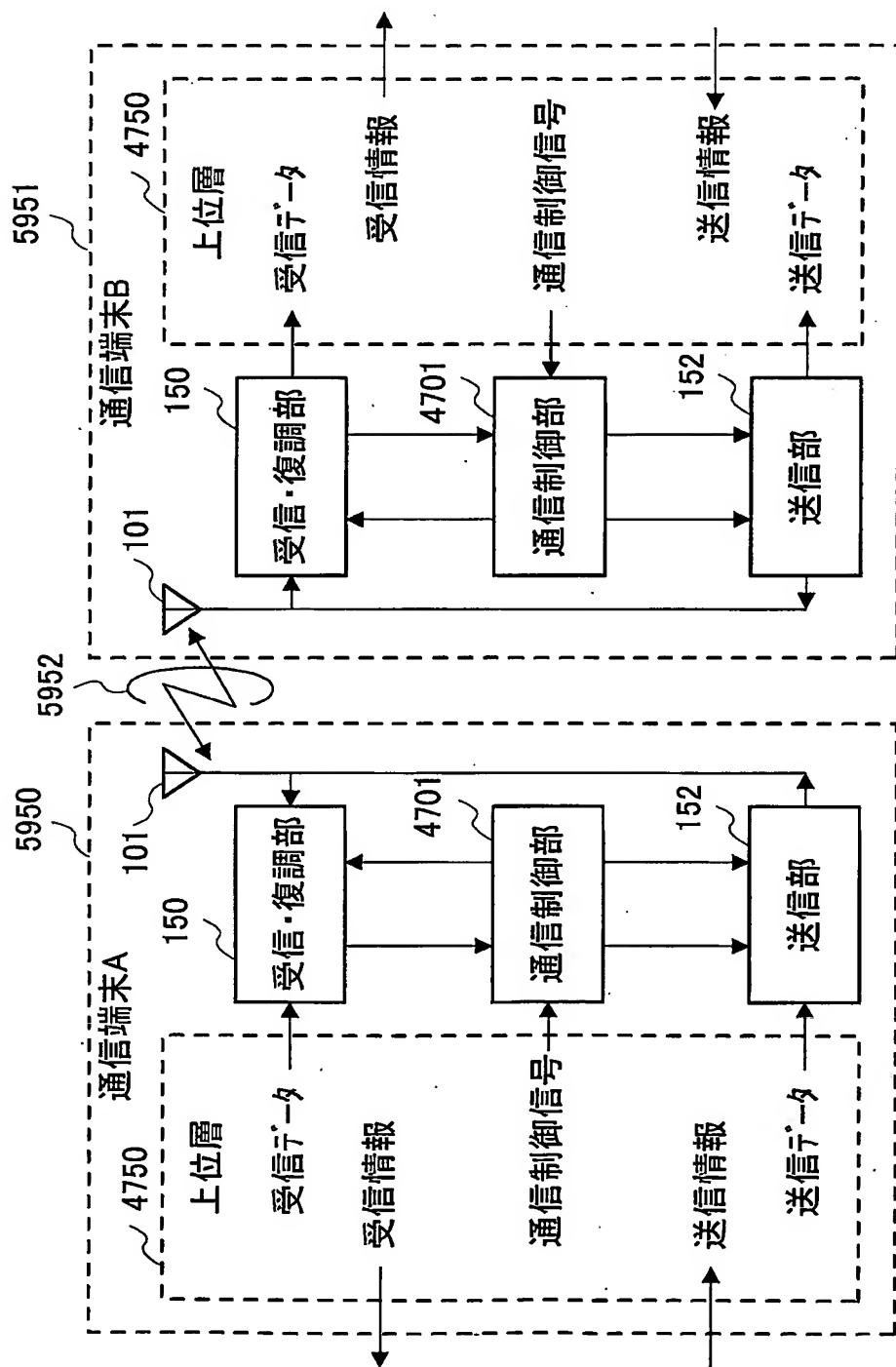


図59

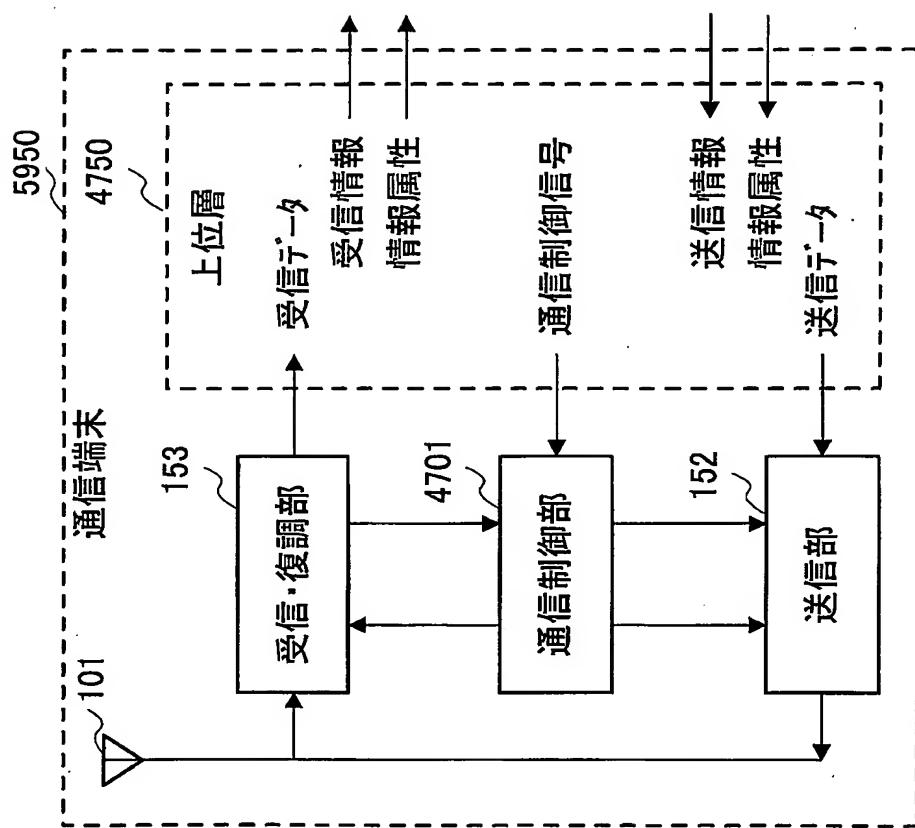


図60

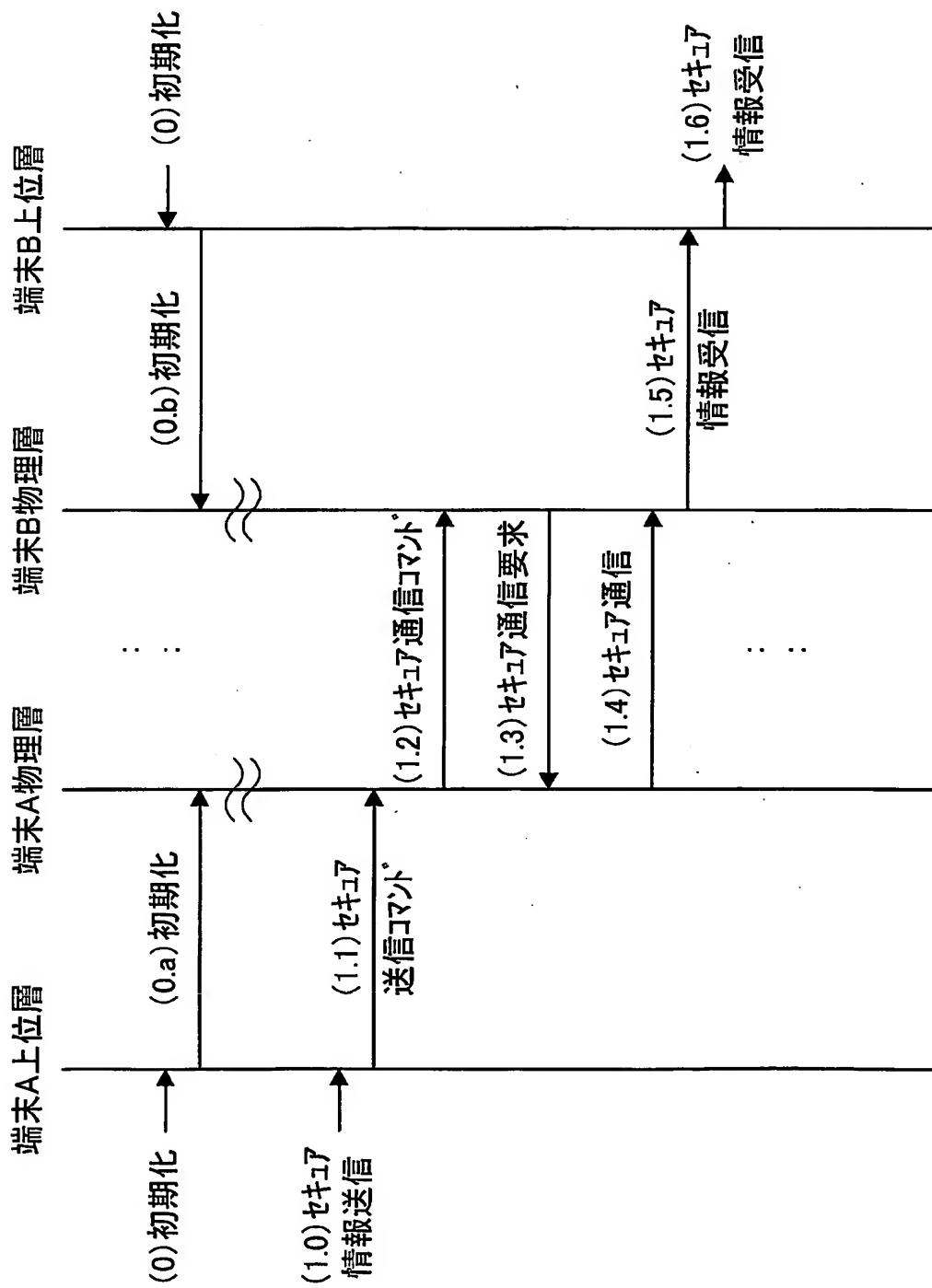


図61

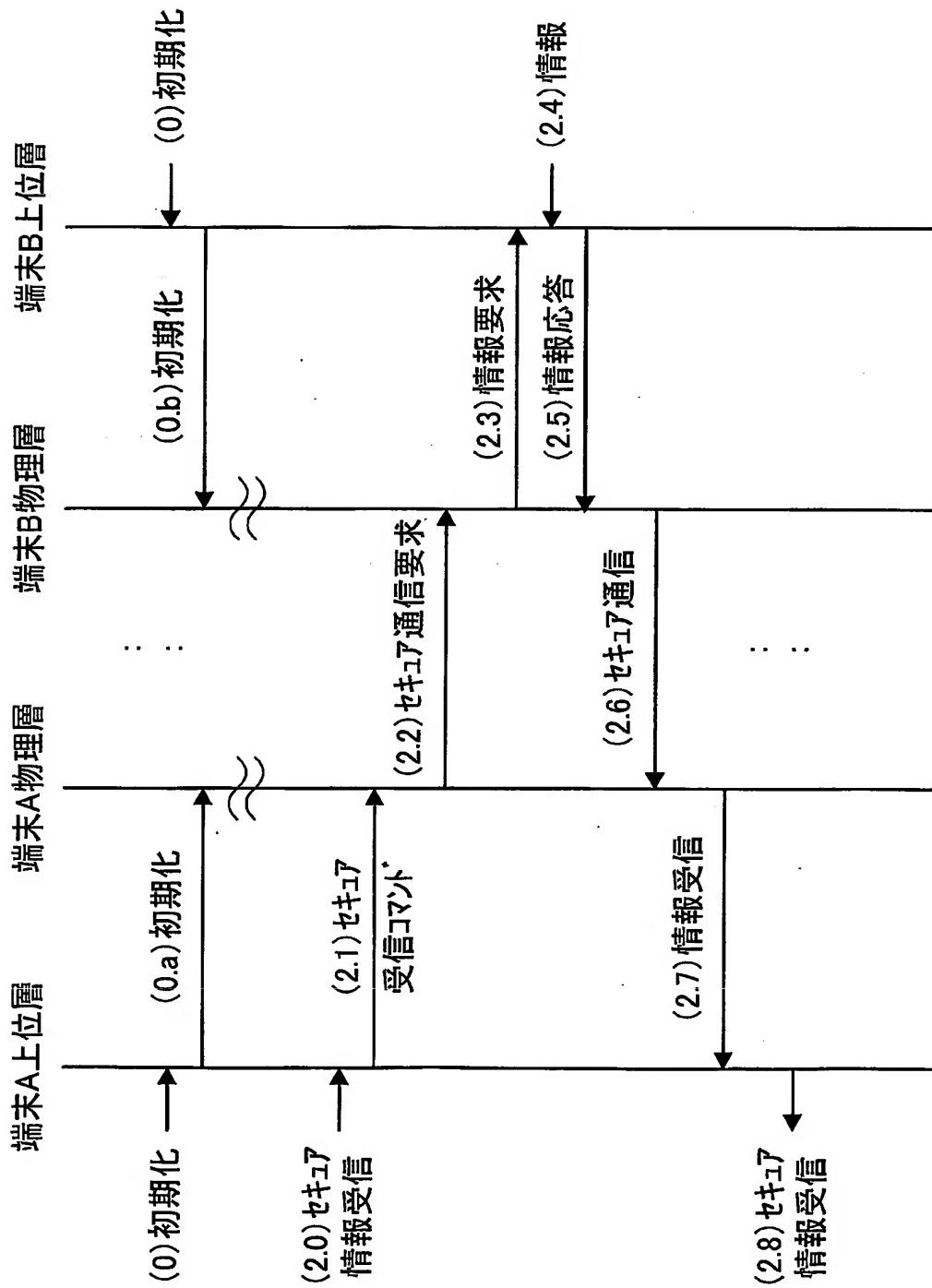


図62

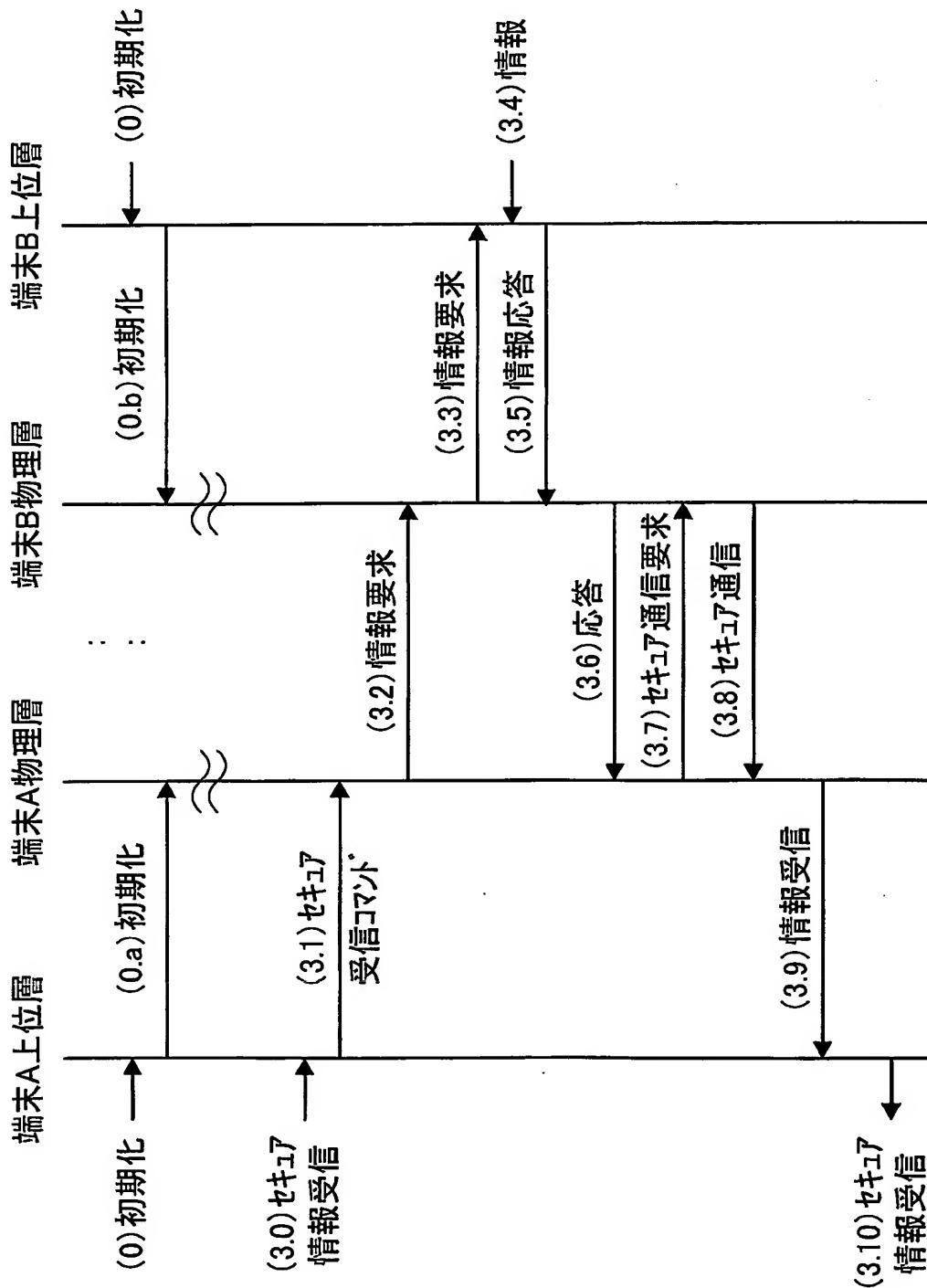


図63

64/78

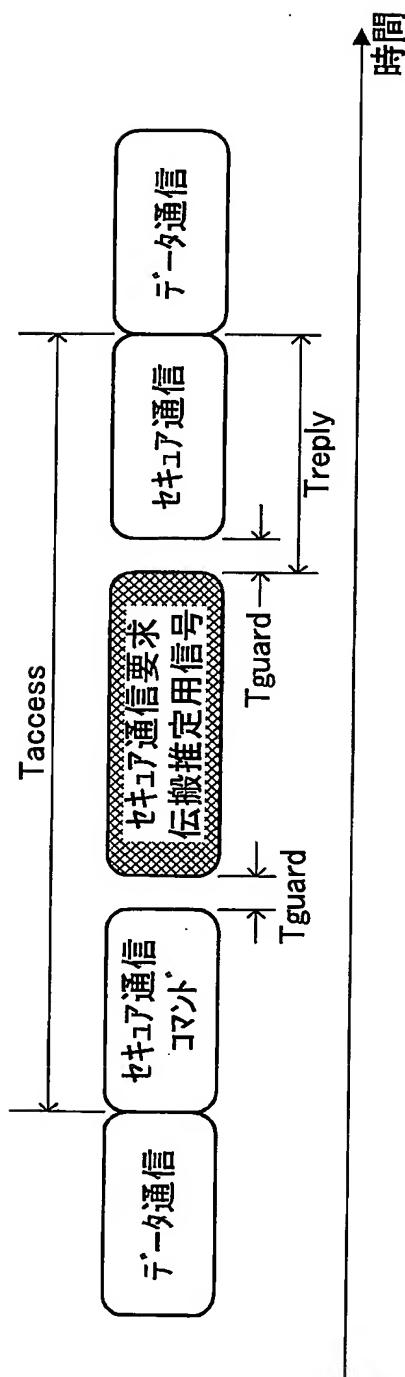


図64

65/78

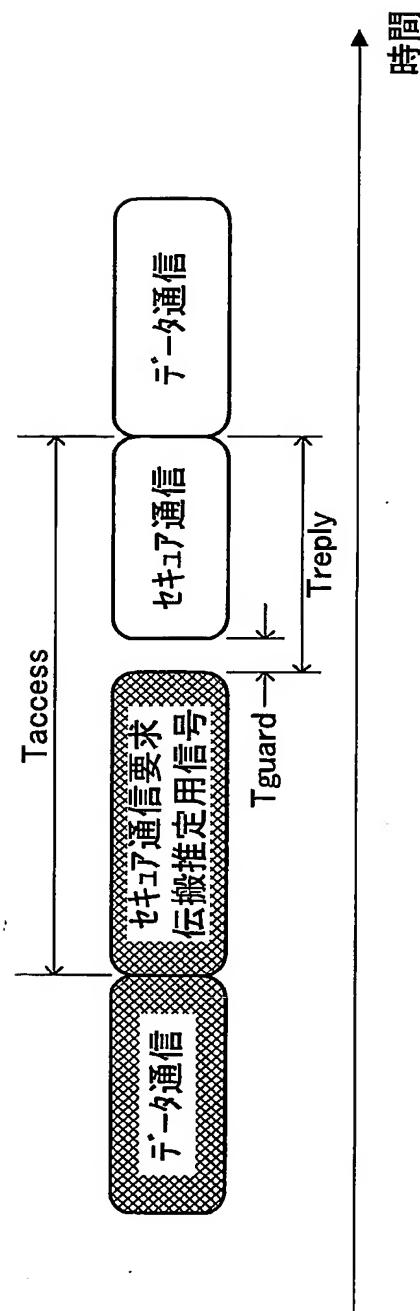


図65

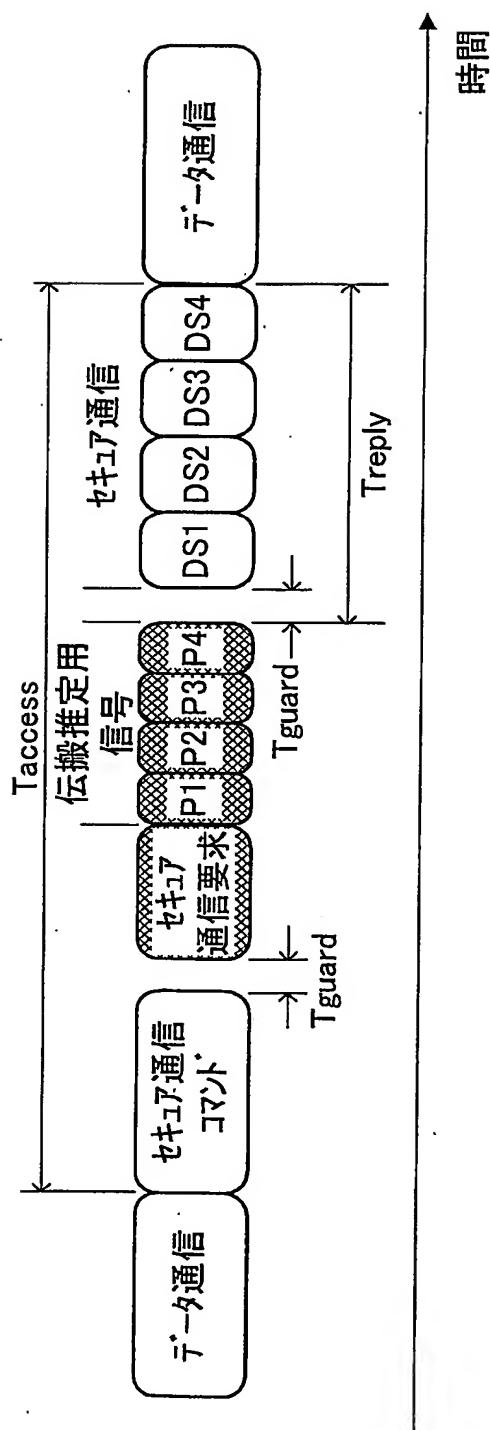


図66

67/78

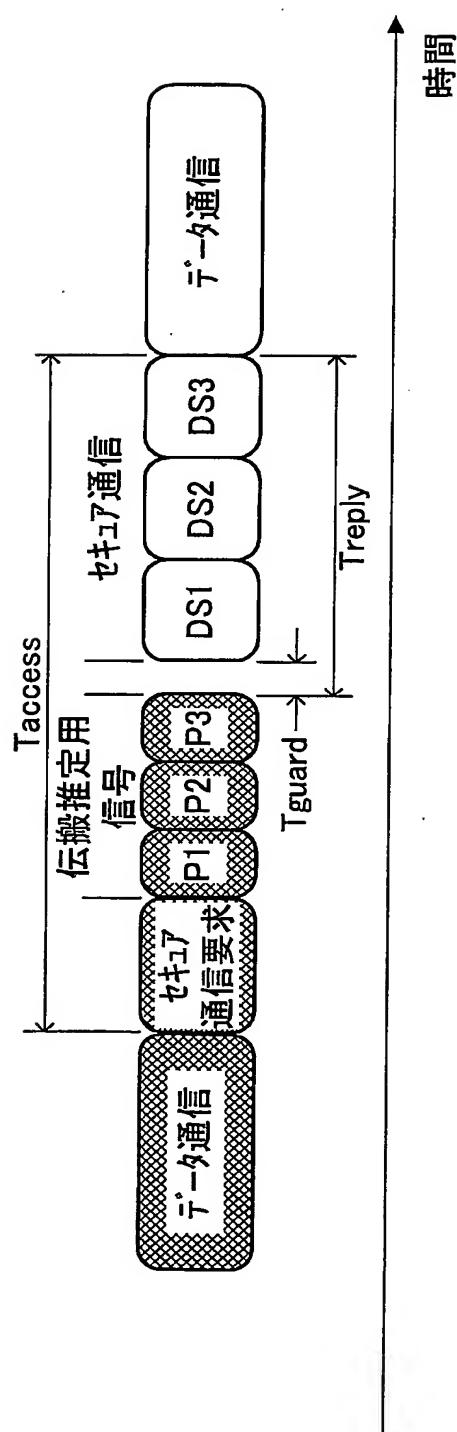


図67

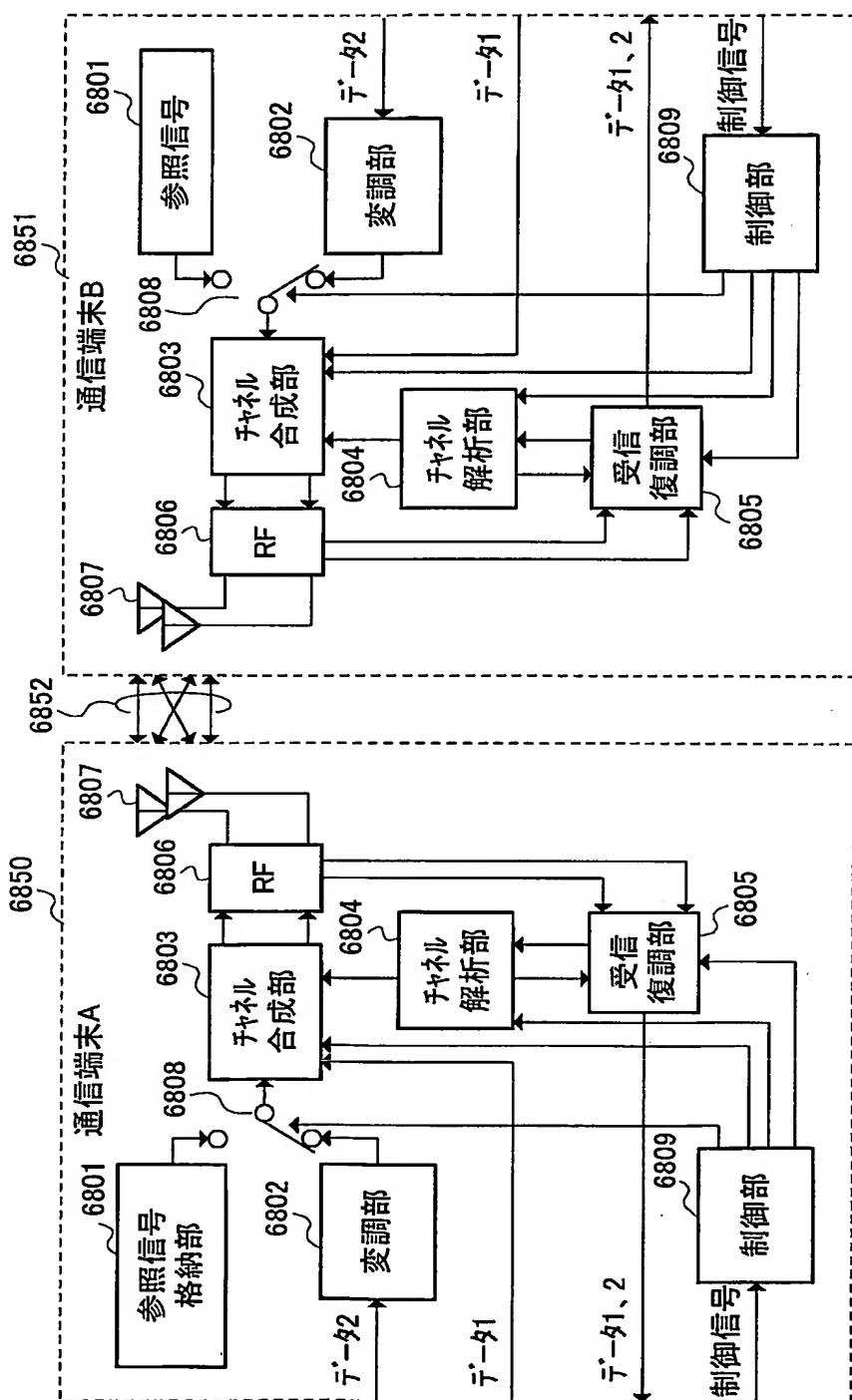
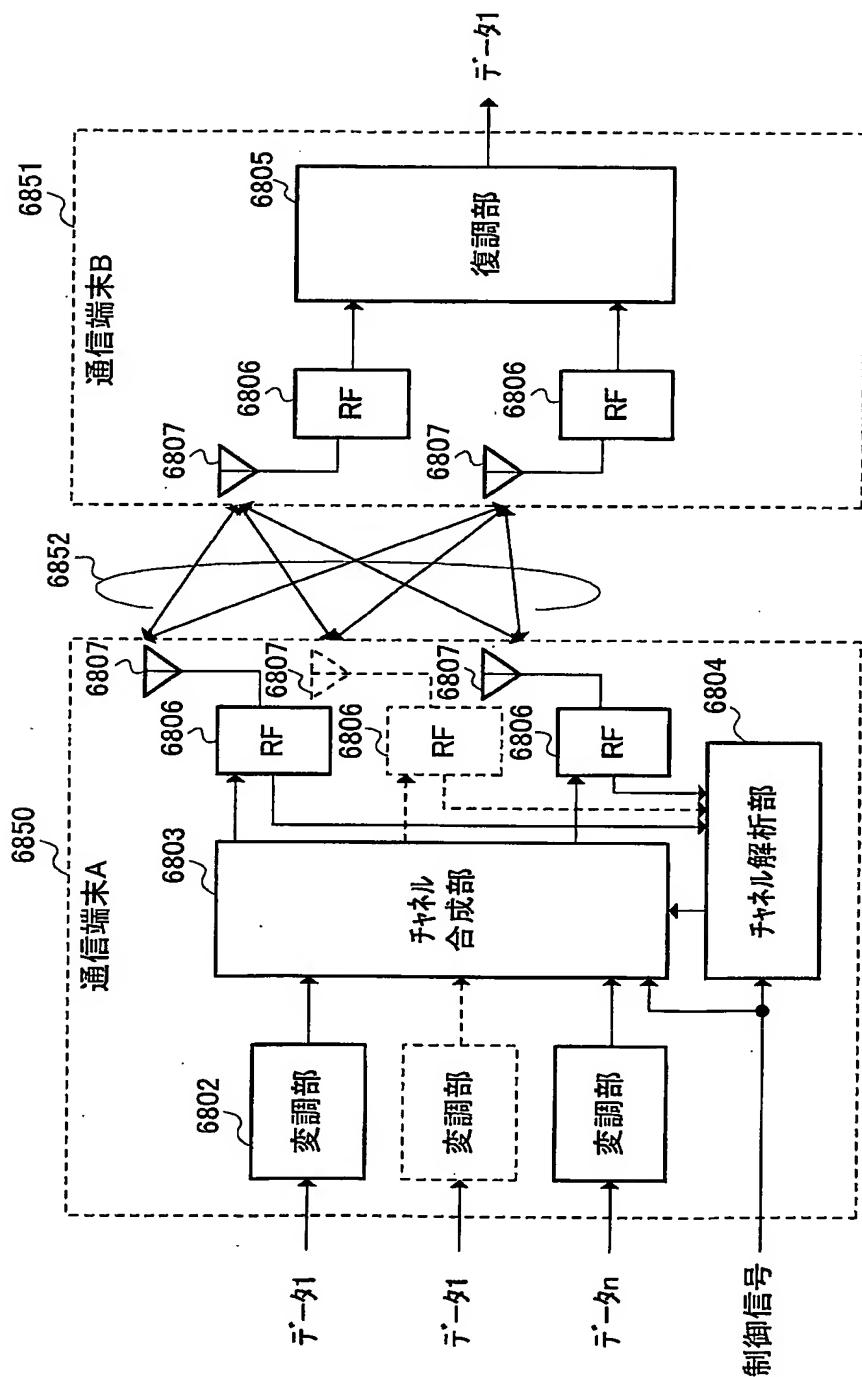


図68



69

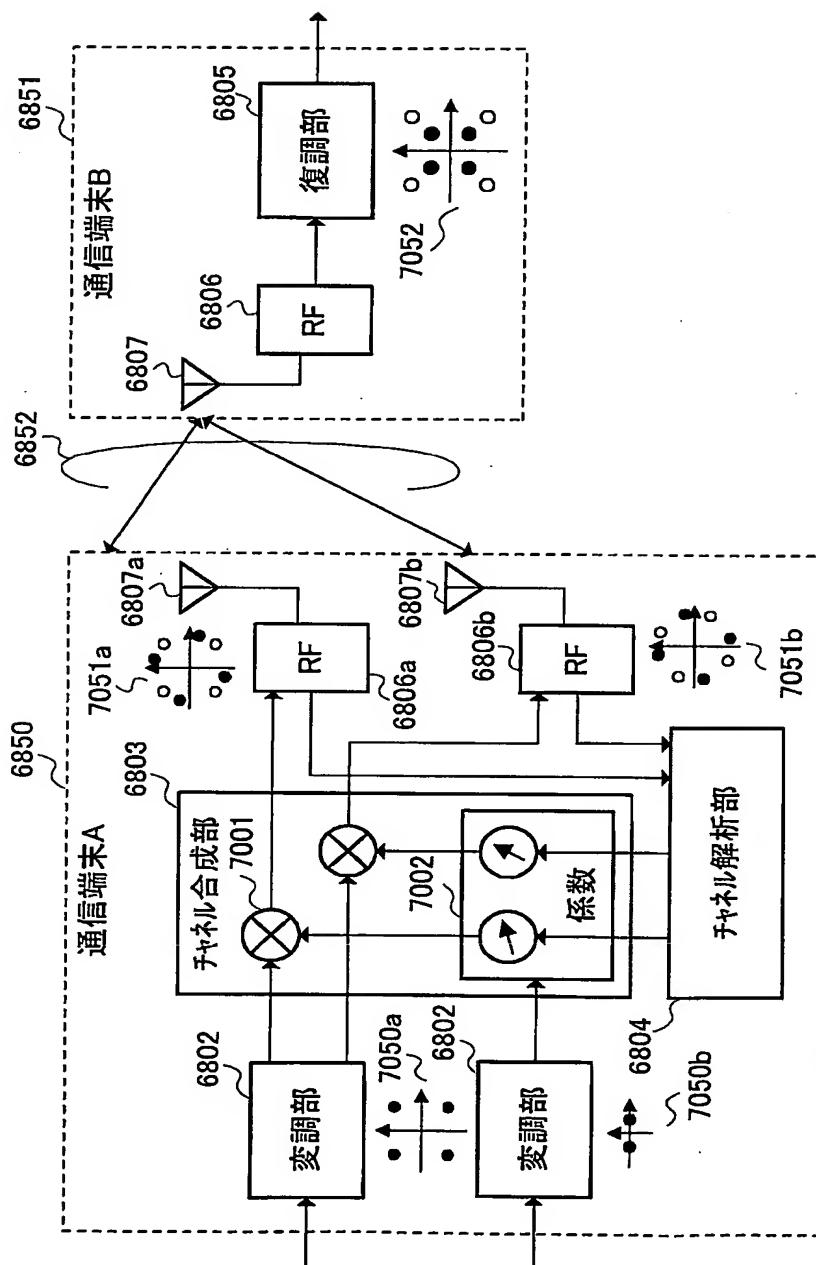


図70

71/78

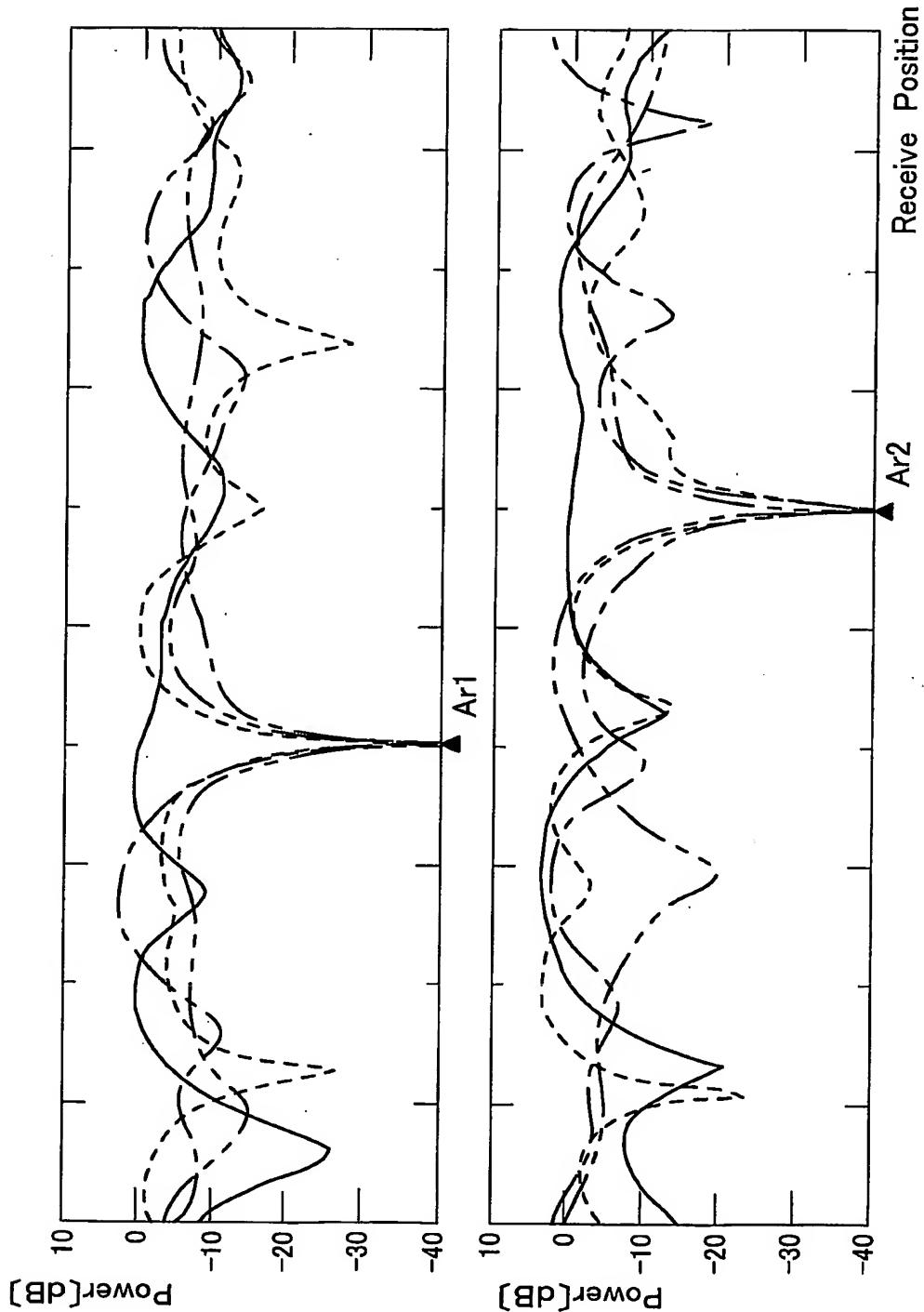


图71

72/78

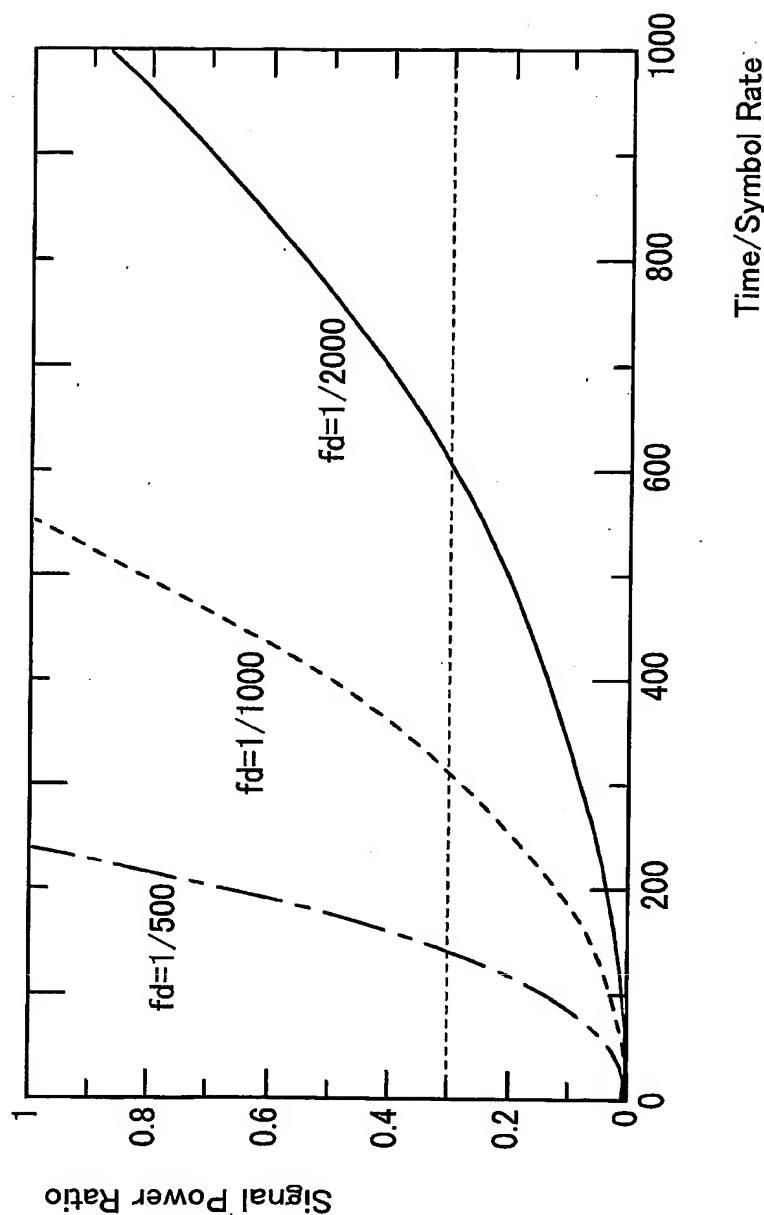


图72

73/78

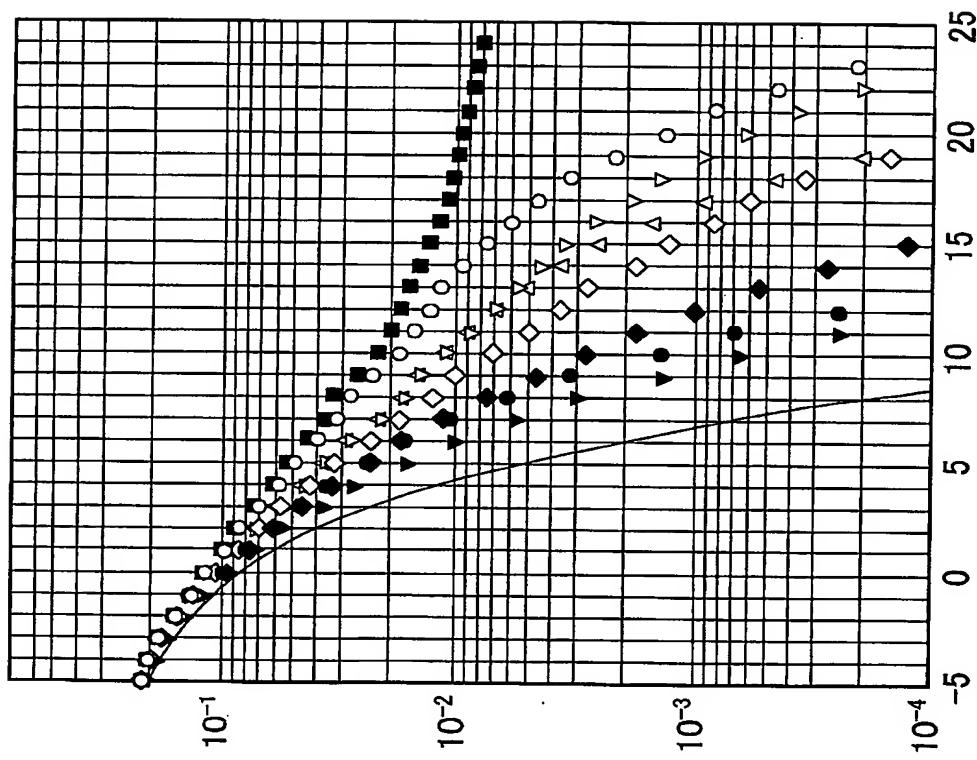


图73

74/78

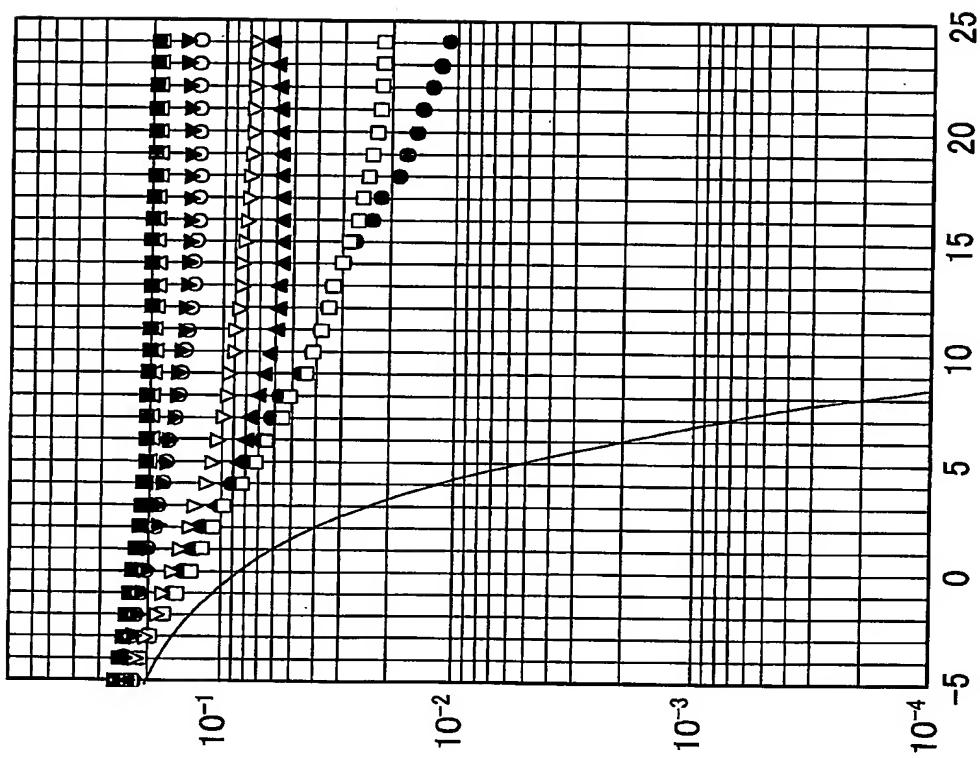


图74

75/78

P1	P2	P3	P4	$\bar{\tau}_1 \bar{\tau}_2 \bar{\tau}_3 \bar{\tau}_4$			
1	2	3	4	$\bar{\tau}_1 \bar{\tau}_2 \bar{\tau}_3 \bar{\tau}_4$			
$d_{11} + d_{22} + d_{33} + d_{44}$	$d_{11} + d_{22} + d_{33} + d_{44}$	$d_{11} + d_{22} + d_{33} + d_{44}$	$d_{11} + d_{22} + d_{33} + d_{44}$				
$v_{11} + v_{22} + v_{33} + v_{44}$	$v_{11} + v_{22} + v_{33} + v_{44}$	$v_{11} + v_{22} + v_{33} + v_{44}$	$v_{11} + v_{22} + v_{33} + v_{44}$				
$d_{11} + d_{22} + d_{33} + d_{44}$	$d_{11} + d_{22} + d_{33} + d_{44}$	$d_{11} + d_{22} + d_{33} + d_{44}$	$d_{11} + d_{22} + d_{33} + d_{44}$				
$v_{11} + v_{22} + v_{33} + v_{44}$	$v_{11} + v_{22} + v_{33} + v_{44}$	$v_{11} + v_{22} + v_{33} + v_{44}$	$v_{11} + v_{22} + v_{33} + v_{44}$				

図75

76/78

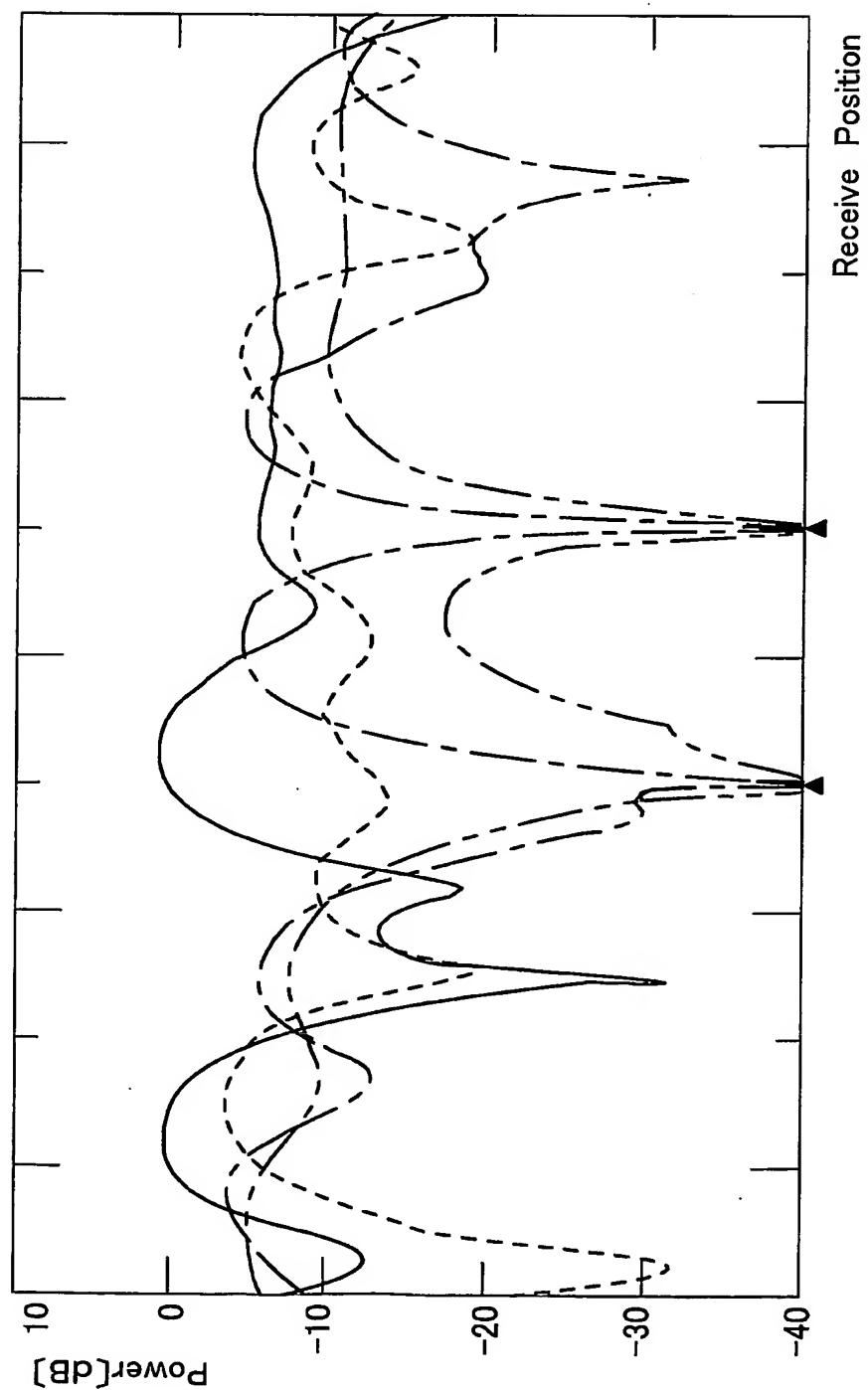
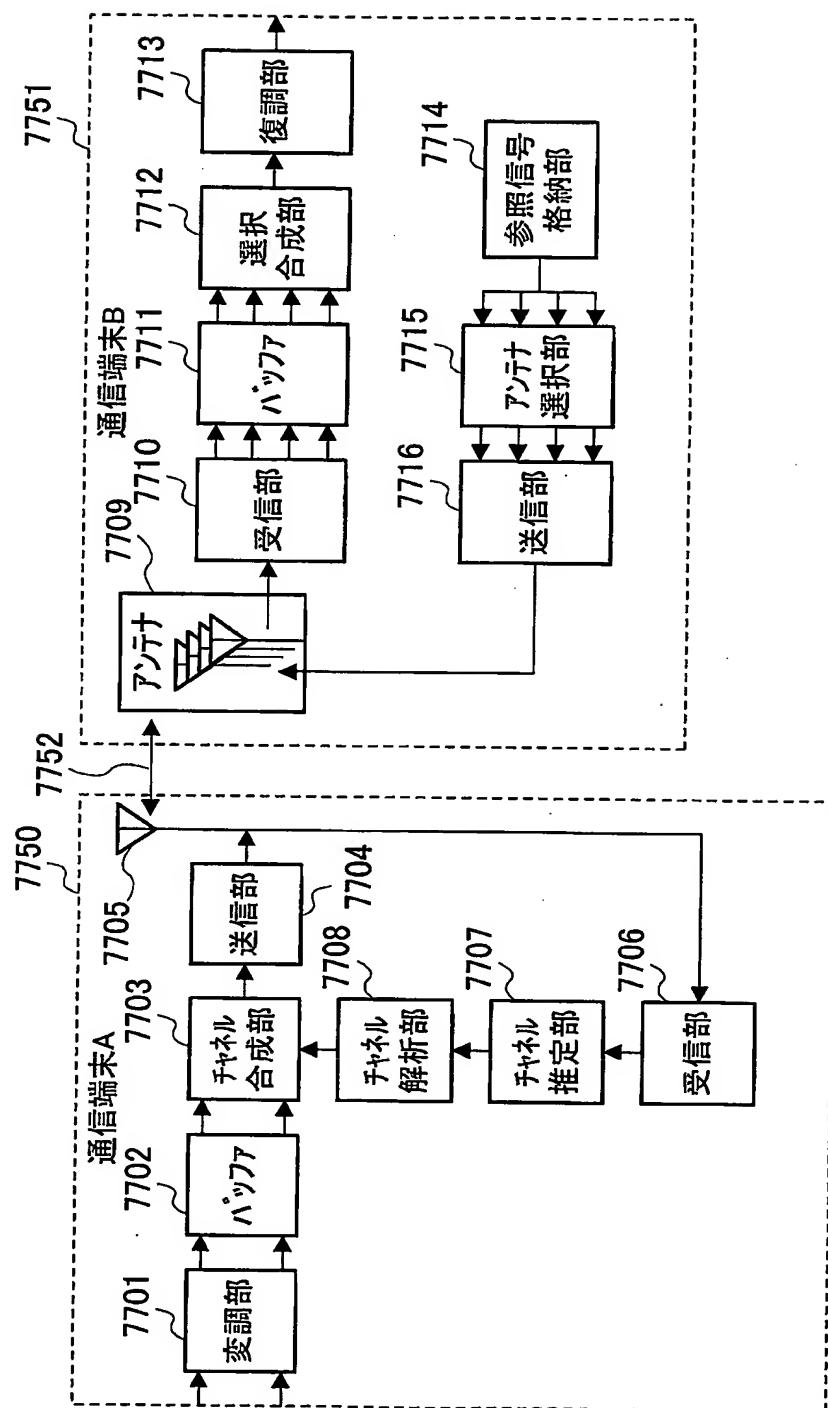


图76

77/78



77

78/78

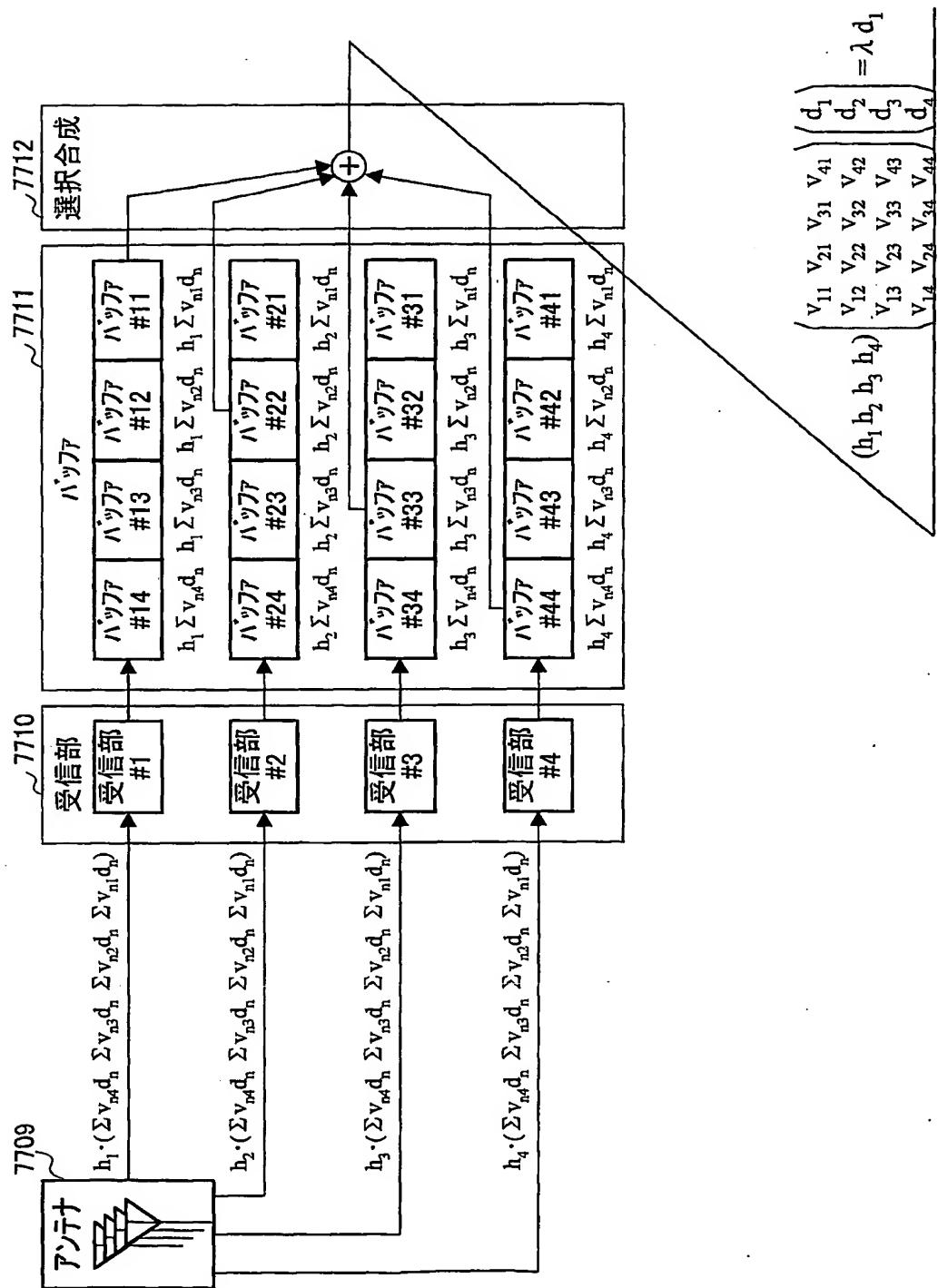


図78

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/02174

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/08, H04L9/14, H04Q7/38, H04B7/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/08, H04L9/14, H04Q7/38, H04B7/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
 Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2003
 Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Chikako UCHIYAMA, "Ryoshi Rikigaku no Kiso to Ryoshi Ango Ryoshi Tsushin Channel no Shiten", Surikagaku, The December issue, Saiensu-sha Co., Ltd., No.402, 01 December, 1996 (01.12.96), pages 53 to 61	1-3,12
X	Masayoshi MUROYA, Heichi YAMAMOTO, "Digital Communication Series Digital Musen Tsushin", Sangyo Tosho Kabushiki Kaisha, 5th edition, 10 March, 1992 (10.03.92), pages 103 to 127	1,3-9,11
Y	pages 169 to 170	10
Y	JP 5-41607 A (KDD Kabushiki Kaisha), 19 February, 1993 (19.02.93), Full text; Figs. 1 to 9 & US 5218359 A	10

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"E" earlier document but published on or after the international filing date

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"O" document referring to an oral disclosure, use, exhibition or other means

"&" document member of the same patent family

"P" document published prior to the international filing date but later than the priority date claimed

Date of the actual completion of the international search
22 May, 2003 (22.05.03)

Date of mailing of the international search report
03 June, 2003 (03.06.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Faxsimile No.

Telephone No.

A. 発明の属する分野の分類(国際特許分類(IPC))

Int. Cl' H04L9/08 H04L9/14 H04Q7/38 H04B7/06

B. 調査を行った分野

調査を行った最小限資料(国際特許分類(IPC))

Int. Cl' H04L9/08 H04L9/14 H04Q7/38 H04B7/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2003年
日本国登録実用新案公報	1994-2003年
日本国実用新案登録公報	1996-2003年

国際調査で使用した電子データベース(データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	内山智香子：“量子力学の基礎と量子暗号 量子通信チャンネルの視点”，数理科学 12月号，株式会社サイエンス社，NO. 402, 1996. 12. 01 p. 53-61	1-3, 12
X	室谷正芳, 山本平一：“デジタル コミュニケーション シリーズ デジタル無線通信”，産業図書株式会社，第5版，1992. 03. 10 p. 103-127	1, 3-9, 11
Y	p. 169-170	10

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示すもの
- 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す)
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日

22. 05. 03

国際調査報告の発送日

03.06.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官(権限のある職員)

青木 重徳



5M 4229

電話番号 03-3581-1101 内線 3597

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 5-41607 A (国際電信電話株式会社) 1993. 02. 19 全文, 図1-9 & US 5218359 A	10